CYBERCRIME IN PAKISTAN: A STUDY OF THE LAW DEALING WITH CYBERCRIMES IN PAKISTAN

MARIA AKHLAQ[ϕ]

[ϕ] Maria Akhlaq is an alumni of Pakistan College of Law where she completed University of Punjab's LLB programme.

ABSTRACT

Cybercrime is a criminal act committed using digital devices and the internet. With the whole paradigm of every human activity shifting towards technology, criminal activities committed through these technological means also have increased manifold. Lack of awareness regarding the issue of cybercrime has caused many difficulties. Pakistan did not have any specialised legislation until the passage of the Prevention of Electronic Crimes Act, 2016. This paper analyses cybercrime, it's meaning and forms, the complexity it presents, and its situation in Pakistan. It also critically analyses PECA and how cyber law in Pakistan is a means to stifle the freedom of speech in Pakistan. Lastly, it provides recommendations as to how the current cyber law can be improved.

INTRODUCTION

Everything in the universe follows the process of evolution and revolution. The common goal of both processes is simply 'change'; it may be good or bad depending on the subject being studied, but it is inevitable, and nothing can stop it. With it, ideas become ideas and then rules, and in time these laws are broken, and new ones are added. There was a time when the earth was designed to be in the center of the earth, and now everyone is convinced that according to modern cosmology, the previously thought-out version of the universe is inaccurate in terms of reference framework. The start of nuclear studies began with the dream of free and clean energy, and generations of scientists worked to understand how to extract and control the forces that lead to nuclear fusion, but this was later used for destructive purposes and became a weapon of war and mass destruction. The same cycle sadly repeats itself in the event of modern digital technology, through the invention/development of the internet. The ultimate goal of this development of technology was to establish ways to share information and keep people around the world more connected and updated. The founder of the internet is the English scientist 'Tim Berners-Lee' who developed a brilliant and revolutionary concept to join different networks together and share files and data between them. He is regarded as the inventor of the 'World Wide Web' or simply 'WWW.'[1] Emails have been around since the 1960s, and file-sharing began in the 1970s. The year 1989 marked the proper launch of the world wide web. It should be noted that nuclear power in the wrong hands can kill and destroy. Similarly, the internet can be used to destroy and damage. The difficulties and consequences may vary, but in all cases, the damage is done. The technology itself is not bad, and its users decide whether it will be used for good or bad. As social networking and social / entertainment

[1] 'A Short History of the Web' (*CERN)* <https://home.cern/science/computing/birth-web/short-history-web> accessed April 19, 2021

opportunities began to flood the internet, people began to be drawn to them, and usage skyrocketed. It is estimated that in Pakistan alone, internet usage is between 2 TBps and 4 TBps, meaning that at one moment, the data exchanged on the internet is at least two terabytes (1 Terabyte = 1024 GigaBytes). It cannot be assumed that all this information was shared solely for great benefit. This information sharing has far-reaching effects and sometimes negative too.

The crime scene in today's world has changed, and we now have a new name known as 'Cyber Crime,' which simply means that crimes committed using computers or new internet-based technologies.

I. THE GROWTH AND CONTEMPORARY USE OF INTERNET

Cybercrime cases did not start suddenly. In fact, they emerged with the passage of time and with technology surpassing the ideas of the previous generation. The growth of computer innovation is descriptive and complex as well. People in developed countries where literacy rates were high quickly adopted new technologies and equipped themselves with modern devices and standards. However, people with a low level of education and a limited understanding of technology initially had reservations about the use of technology in their daily activities, but gradually the comfort of technology and digital applications was adopted, and soon technology found its way into corporate offices. The old methods of storing physical files have been replaced by current domain systems and cloud-based programs today. The goal of the cloud is simply that user or partner information is stored on an online distribution server or, in other words, 'computer storage and processor.'

One of the most popular forms of digital use is the digital presence of the local community on social media. Social networking platforms

are also introduced to people so that they stay connected to friends and family and may meet new people. The dream of making the world a global city was the focal point of social media. These social media platforms have hit the global community like thunderstorms, and everyone, regardless of gender, religion, region, class, and creed, has joined these platforms.

With a platform being digitally accessible to every kind of person, the concept of cybercrime turned into a vicious and disgusting phenomenon. These platforms are inherently free to use and accepted by everyone to share their personal information such as photos, videos, and contact information hence opening windows for their misuse, also constituting cybercrime. As the article progresses, it becomes apparent how serious this problem is.

The Digital revolution has also brought many opportunities for leadership and livelihoods. These days apart from technology-based opportunities, content creation opportunities are available for the general public.

The cycle is simple:

- People make digital content (videos, articles, images, etc.).
- Digital content is uploaded on content sharing platforms (social media and others).
- The general public watches or reads the content.
- Advertisements are displayed on the content.
- The more the views, the more the earning for the creator and the platform.

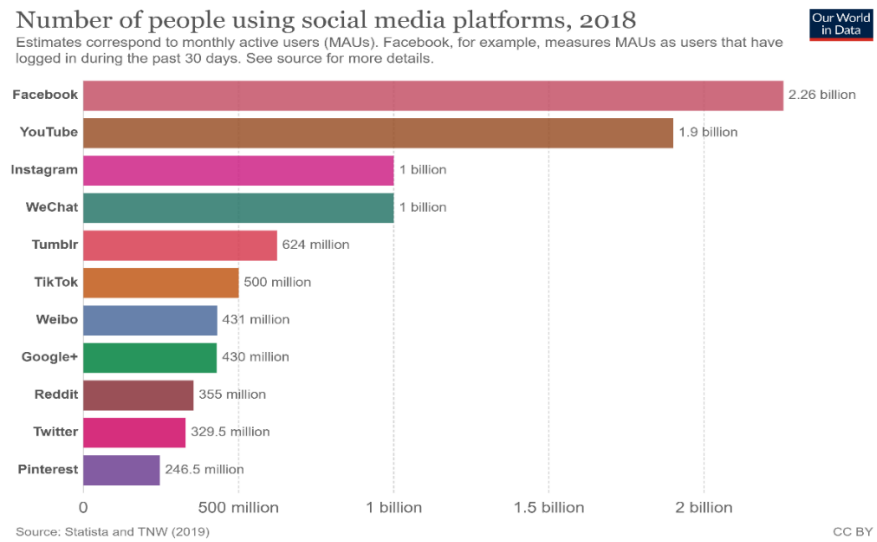

Figure 1 Stats of Social Media Users Globally

This proved to be very beneficial in the start, as it provided people with earning opportunities within the comfort of their homes. The issue started with the quality of the content and its moderation. Content moderation is a very potent issue. The content of creators would and could be offensive to some specific groups or contain fake or false information causing unrest in the society, which could result in disastrous outbreaks of protests and sometimes financial damages or defaming. The demand of digital content has increased very much, and targeted digital marketing campaigns have benefitted many businesses more than traditional marketing campaigns.

However, the dark side of this content creation can be observed in the adult film or porn industry of the world. There are thousands and thousands of adult content websites available over the internet today, which contain sexual as well as bizarre videos and images of actors, feeding bad and erotic ideas into the minds of its viewers. This industry is totally dependent on the bulk of content each website publishes, and with more views, they earn more; hence the cycle continues. The corrupt amongst the society have sought to use these platforms as an earning source by using illegal footage and forced

pornography. Details of this would be discussed as the article progresses.

Pakistan does not suffer more from the traditional form of cybercrimes involving digital theft, frauds, etc., but it suffers more from digital content-based crimes and other malicious acts like blackmail, impersonation, and defamation/fake news and unauthorised usage of data. The legislation to curb these cyber crimes is rather primitive in Pakistan, even though recent legislation on the subject, however lacking, has still been a step forward. FIA currently acts as the legal body to deal with cybercrimes. It reported that in 2017 it received only 1290 inquires[2]; this number is very less as most of the population is unaware of how to register cybercrimes, and a campaign to educate the public is needed for this as well. We will discuss the loopholes in the laws (PECA) and their incompleteness. It will become apparent that new and more vigilant reforms are needed to control this rising form of crime.

II. CYBERCRIMES: AN OUTLINE

The first and foremost problem that the term cybercrime presents is the absence of a proper and absolute definition. Cybercrime is generally described as "a generic term that refers to all criminal activities done using the medium of computers, the internet, cyber space and the worldwide web"[3]. This definition is somewhat lacking as it leaves out a lot of other means by way of which cybercrimes can be committed e.g mobile phones.

---

[2] Shakeel Qarar, 'Cybercrime reports hit a record high in 2018: FIA' The *Dawn* (October 23, 2018) <https://www.dawn.com/news/1440854> accessed 16 March 2021.

[3] Prashant Mali, *A Text Book of Cybercrime and Penalties* (Indiana: Repressed Publishing LLC, 2006) 3

In a rather comprehensive definition, it is defined as "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 harm to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)"[4]. This definition is much wider as it expands the scope of means by which such criminal activities can be committed and also takes into account the criminal intent behind those activities.

In Pakistan, the authority that deals with cybercrime matters is Federal Investigation Agency (FIA). The FIA defines cybercrime on its official website as "any activity commissioned via computer, digital devices and networks used in the cyber realm, and is facilitated through the internet medium."[5] It includes distant theft of information belonging to an individual, government or corporate sector through criminal tress-passing into unauthorized remote systems around the world. It includes stealing from online banks to harassing and stalking cyber users. Cybercrime also includes sending viruses on different systems, or posting defamatory messages.

The term "Cybercrime" is also used synonymously with "technological crime", "digital crime", "high tech crime" etc. So, in order to understand the phenomenon that is cybercrime, one must consider its characteristics rather than a definition.

Broadly speaking, all those illicit activities which are committed through some digital and technological means can be covered under the umbrella of cybercrime and where the 'common denominator' is the central role played by networks of information and communication technology"[6]

---

[4] DH Jaishankar, "Cyber Crime and the Victimization of Women: Laws, Rights and Regulations" (2012) Hershey: Information Science Reference.

[5] 'Federal Investigation Agency' <http://fia.gov.pk/en/NR3C.php> accessed May 2, 2021.

[6] Majid Yar, *Cyber Crime and Society* (London: SAGE Publications Ltd, 2006) 9

There are two major categories of cybercrime. In one, the computer is the target of the offence; attacks on network confidentiality, integrity and/or availability—i.e., unauthorised access to and illicit tampering with systems, programs or data—all fall into this category.

The other category consists of traditional offences—such as theft, fraud, and forgery—that are committed with the assistance of or by means of computers, computer networks and related information and communications technology; here, the computer is a tool used to commit a conventional crime[7].

THE COMPLEXITY OF CYBERCRIMES

Words and phrases that scarcely existed a decade ago are now part of our everyday language, as criminals use new technologies to commit cyberattacks against governments, businesses and individuals. These crimes know no borders, either physical or virtual, and cause serious harm and pose very real threats to victims worldwide

Technological advances are increasing rapidly and these advancements have also created myriad opportunities for offenders to commit various forms of crime. These Cybercriminals are exploiting these new technologies with lightning speed and tailoring their attacks using new methods. The reason being their skill and knowledge of these technological intricacies which they are able to decode. Cybercrimes occur because 'the perpetrator uses special knowledge of cyberspace.'[8]

---

[7] Marc D. Goodman, "Why the Police Don't Care About Computer Crime" (1997) 10 HARVARD J. LAW & TECH. 465, 468–469.

[8] S Furnell, *Cyber Crime: Vandalizing the Information Society* (London: Addison Wesley 2002).

The reason why cybercrimes are complex in nature are; firstly, because they involve technological ingenuities which not everyone is able to grasp. Only someone with expert skill is able to decipher the kind of nuances which cybercrime presents. The law enforcing agencies and the authorities often lack the expertise to deal with the matter of cybercrime and investigate them properly. "One of the reasons is that cyber forensic facilities are not available. The forensic system is direly required to cope with digital crimes."[9]

Secondly, apprehending a cybercriminal and evidence collection in cases of cybercrime are extremely challenging for the authorities as someone who commits that kind of complex crime often knows how to eliminate evidence of his nefarious activities and the criminals often evade. Oftentimes, especially on larger scales, when cybercrime is committed, there is seen a whole network of such criminals who act in a very coordinated manner and they make very intricate attacks in a matter of minutes. In such cases, it is even harder to apprehend the perpetrators and collecting evidence. In some cases, the difficulty in apprehending offenders is due to the offenders not being within the national borders or because they are working secretly. For this purpose however, Interpol has established its National Centre Bureau (hereinafter NCB) in its 194 member states. Pakistan is also a supporting member and has its NCB at Islamabad. Combatting cybercrime is one of Interpol's main crime programme by which it aims at providing a safe cyberspace for all its member countries and investigating cyber attacks.

MAJOR PREVALENT CYBERCRIMES

Cybercrimes range from economic offences—such as computer fraud, theft, forgery, industrial espionage, sabotage and extortion, product piracy, and other crimes against intellectual property—to infringements of privacy, the propagation of illegal and harmful

[9] T Kumar, RK Jha, and SM Ray, "Cyber Crime And Thier Solution" (2012) 1 International Journal Of Engineering And Computer Science 48-52.

content, the facilitation of prostitution, and other offences against morality, and organised crime[10]**.** As has been explained before, there is no exact definition of what a cybercrime will be. However, some range of activities that have been considered cybercrime are:

Hacking: Hacking is the unauthorised access to or control over computer network security systems for some illicit purpose. Simply put, misuse of a computer system to break the security of another computer, mostly for the purposes of stealing data, is categorised as hacking. In Pakistan, recent statistics have shown that hacking is quite a trend; from hacking Facebook accounts to hacking into the information system of banks and organisations, hacking is one of the most prevalent cybercrime in Pakistan.

Fraud: Fraud represents the largest kind of cybercrime. The internet has created the opportunity for borderless fraud. The range of what is deemed as fraud is quite extensive. Where an online seller fraudulently sells counterfeit products or advertises one thing but sends another or fails to deliver goods after receiving the payment, these are all instances of fraud. From these instances to the large-scale bank frauds, all are covered in the category.

Bank fraud is a white-collar crime. Impersonating to be a bank employee and then taking out personal and financial information from bank account holders, setting up a fake financial institution, and then luring people into deposit funds, getting fraudulent loans, etc., are all types of bank frauds.

Cyberbullying and harassment: bullying and harassment using electronic means are known as cyberbullying and cyber harassment. These instances can take place over social media, message platforms, gaming platforms, etc. In Pakistan, these cases happen quite often. Especially women are made subject to harassment on online

[10] Marc D Goodman, Susan W Brenner, "The Emerging Consensus on Criminal Conduct in Cyberspace*"* (2002) 10 Int J Law Info Tech 139.

platforms. In 2018-2019, blackmailing and harassment were the most reported cybercrimes.[11]

Cyberstalking: it is a form of stalking done via the internet or digital devices with a motive to intimidate or harass someone by constantly contacting them. These activities are targeted at a person, and the victims usually feel a sense of fear and apprehension. In Pakistan, women are especially prone to stalking and harassment both offline and online.

Digital piracy: Digital piracy refers to the illegal act of duplicating, copying, or sharing a digital work without the permission of the copyright holder, a violation of copyright laws[12] This is a severe violation of the Intellectual property rights of the IP holders. It causes a great loss and hurts businesses, and helps spread malware.

Denial of service attacks: Denial of Service attacks refers to a cyber attack in which the target is the computer or any other device, and they are made inaccessible to their intended users by interrupting the normal functioning of the device.[13] Pakistani websites are routinely attacked with distributed denial of service (DDoS) attacks, making the websites unavailable to visitors where attackers direct a huge amount of traffic using bots or software performing automated tasks. These types of attacks intensify on or around 14 August, which sources say, originate majorly from India.[14]

---

[11] Allia Bukhari, 'Silent Battles: How Pakistani Women Counter Harassment in Cyberspace' *The Diplomat* (21 October 2020) <https://thediplomat.com/2020/10/silent-battles-how-pakistani-women-counter-harassment-in-cyberspace> accessed 17 March 2021.

[12] Jason R. Ingram, 'Digital piracy' *The Encyclopedia of Criminology and Criminal Justice* (2014).

[13] 'What Is a Denial-of-Service (DoS) Attack?' (*Cloudflare*) <https://www.cloudflare.com/en-gb/learning/ddos/glossary/denial-of-service/> accessed May 2, 2021.

[14] Talha Khan, 'Cybercrimes: Pakistan lacks facilities to trace hackers' *Express Tribune* (01 February 2015) <https://tribune.com.pk/story/831178/cybercrimes-pakistan-lacks-facilities-to-trace-hackers > accessed 17 March 2021.

Spoofing: Spoofing is the act of disguising a communication from an unknown source as being from a trusted source. Spoofing can apply to emails, phone calls, and websites or can be more technical, such as a computer spoofing an IP address or Domain Name Servers (DNS).[15] In PECA, it is defined as, "Whoever with dishonest intention establishes a website or sends any information with a counterfeit source intended to be believed by the recipient or visitor of the website, to be an authentic source commits spoofing." And is punishable by imprisonment up to 3 years or fine or both.

Cyberterrorism: Cyberterrorism has been defined as a 'premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against non-combatant targets by subnational groups or clandestine agents.'[16] Cyberterrorism attacks can take many forms. To give an example, An attacker might hack into a domestic banking computer system and disrupt its working, or he might take control of the air traffic control system, manipulating it and causing the planes to crash and collide[17]. All are forms of cyberterrorism

In PECA, cyberterrorism is made punishable with imprisonment up to 14 years or a fine of up to 50 million rupees or both.

Phishing: Phishing is a criminal practice in which targets are contacted by email, phone, or text messages by someone posing as a legitimate or authentic institution to lure people in to provide their personal and sensitive data such as passwords or bank card details etc.

---

[15] Forcepoint. (n.d.). 'What is Spoofing?' < https://www.forcepoint.com/cyber-edu/spoofing > last accessed 17 March 2021.

[16] Mark M. Pollitt, 'Cyberterrorism—Fact or Fancy?', Proceedings of the 20th National Information Systems Security Conference, 285, October 1997 (quoted in Dorothy E. Denning, *Activism, Hacktivism and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*, <http://www.nautilus.org/info-policy/workshop/papers/denning.htm> accessed 17 March 2021.

[17] Marc D Goodman, Susan W Brenner, "The Emerging Consensus on Criminal Conduct in Cyberspace" (2002)10 Int J Law Info Tech 139.

[18] Phishing is one of the most successful kinds of cybercrime due to its tendency to trap individuals easily.

Viruses and malicious software: Viruses are malicious codes that are usually attached to another executable program, and once loaded, they replicate the malicious code and self propagate it to other computers. Once loaded into a computer system, it will damage the files and data present on its hard disk. Under section 20 of PECA, the spreading of malicious code or viruses is punishable with imprisonment up to two years or with a fine of up to one million rupees or with both.

Cyber pornography: Cyber pornography is the practice of using cyberspace to create, display, distribute, import, or publish pornography or obscene materials. Usually, pedophilic materials depicting children engaged in sexual acts with adults are especially disseminated. It is a criminal offence and falls under section 19 of PECA, under offences against the dignity of natural persons and minors. Pakistan has seen a hike in these types of cases in recent years. Recently in December 2020, the FIA cybercrime wing arrested a man for illegally obtaining and sharing child pornography. In the past year, the FIA cybercrime wing announced the arrest of six suspects linked and involved with child pornographic rings. Earlier, such rings were also unearthed in various other cities, including Lahore, Gujranwala, Islamabad, Kasur, Sialkot, Rawalpindi, and Sargodha.[19]

NEED FOR CYBERCRIME LEGISLATION

[18] 'What Is Phishing?' (*Phishing.org*) < https://www.phishing.org/what-is-phishing#:~:text=Phishing%20is%20a%20cybercrime%20in,credit%20card%20details%2C%20and%20passwords > accessed May 2, 2021.

[19] Shakeel qarar, 'FIA arrests man accused of obtaining, distributing child pornography on social media' *Dawn News* (29 December 2020) <https://www.dawn.com/news/1598523/fia-arrests-man-accused-of-obtaining-distributing-child-pornography-on-social-media> accessed 17 March 2021.

Nations around the world are very concerned about cybercrime, a concern that is shared by many international organizations, including the United Nations, the G-8, the European Union and the Council of Europe. There are a number of reasons to be concerned, perhaps the most important of which is the problems law enforcement officers and prosecutors can encounter when they try to apply existing law to criminal activities in cyberspace.[20]

The need for special cybercrime law in nations can be stressed upon by this very notorious case, the ILOVEYOU Virus, also called "Love Bug" virus. This virus was unleashed on May 4, 2000. Victims received an email attachment entitled LOVE-LETTER-FOR-YOU. It contained malicious code that would overwrite files, steal passwords, and automatically send copies of itself to all contacts in the victim's Microsoft Outlook address book. It had infected almost 45 million computers worldwide and caused billions of dollars worth of damage. Virus experts quickly traced its origin to a man named Onel de Guzman in Philippines but since there was no cybercrime law in Philippines and it was not a crime to create and disseminate a virus, despite efforts no one was ever prosecuted for the crime even after the passage of 20 years.

Law enforcement officials cannot take action against cybercriminals unless countries have laws that criminalise the activities in which these offenders engage. As the 'Love Bug' investigators learned, the existence of such laws is a fundamental prerequisite for investigation as well as for prosecution. All of the damage the virus ensued worldwide was the consequence of absence of cybercrime legislation in Philippines.

The need for National legislations on Cybercrime are felt more than ever now and nations all around the world are now taking it

[20] Marc D Goodman, Susan W Brenner, "The Emerging Consensus on Criminal Conduct in Cyberspace" (2002) 10 Int J Law Info Tech 139.

seriously and making specialized laws in regards to the subject in an effort to make cyberspace safe for their people.

III. CYBERCIME AND PAKISTAN

Internet access is available in Pakistan since the mid 90's. Internet users have increased exponentially since then. According to the statistics provided in DataReportal, There were 61.34 million internet users in Pakistan in January 2021. The number of internet users in Pakistan increased by 11 million (+21%) between 2020 and 2021.[21]

With the increase in internet use, the nefarious activities committed online which come under the umbrella of cybercrime has also increased. However, Pakistanis do not pay much attention to cyber issues such are cybercrimes. They are mostly busy with their routine lives. They are generally not aware of the tools of cybercrimes. Pakistan's role in cybersecurity is almost nothing at all. FIA and other bodies are although trying their best to cope with the situations, but things are getting worse[22].

The government of Pakistan has established the "National Response Centre for Cybercrime" under the administrative control of FIA to investigate cybercrimes. It has "expertise in Digital Forensics, Technical Investigation, Information System Security Audits, Penetration Testing and Trainings".[23] . By today, the FIA has established 15 anti-cybercrime centres. However, the 15 centres cover the entire country, and each centre has to deal with the complaints

---

[21] Simon kemp, 'DIGITAL 2021: PAKISTAN' *DataReportal* (11 February 2021) <https://datareportal.com/reports/digital-2021-pakistan> accessed 17 March 2021.

[22] A Ahmed and DS Khan, "Cyber Security Issues and Ethical Hacking in Pakistan" (2015) Department of Computer Science Karachi University.

[23] '*National Response Centre For Cyber Crime*' <http://www.nr3c.gov.pk/> accessed May 2, 2021.

from several districts. For example, the FIA cybercrime centre in Lahore has to investigate the complaints registered across the Lahore and Sahiwal divisions, which include altogether seven districts with a cumulative population of around 27 million residents.

UNDER REPORTING OF CYBERCRIMES

Despite the establishment of cybercrime centres and even an online system of filing complaints, Cybercrimes are not reported in abundance and the most vicious kinds of cybercrimes consisting of bank and credit frauds are the least reported ones. The most reported cybercrimes are of cyber harassment, cyber bullying & defamation. People in Pakistan are mostly not aware of the recent legislations made under PECA. The concept of launching an FIR on the basis of being bullied online is still very foreign and is often thought of as an extra baggage to take, hence the road to ignore such tedious crimes is taken and many perpetuators never come under the grip of law. It is rather a case of unawareness and unwillingness on part of the public that cybercrime remain one of the least reported crime in Pakistan and it is arguably one of most ignored and committed crime in Pakistan as well. According to some statistics provided by the FIA the year wise enquires conducted for cybercrimes are as follows[24]:

Year	No. of inquires	No. of Cases Registered
2016	514	47
2017	1290	207
2018	20295	255
2019	11389	1071

[24] Rizwan shehzad, 'Only 14 cyber crime convictions in five years' *Tribune Pk* (20 July 2020) <https://tribune.com.pk/story/2255771/only-14-cyber-crime-convictions-in-five-years> accessed 17 March 2021

It was also revealed that only 14 convictions were made in 5 years (2015-2019), this raises a question mark on the effectiveness of PECA as a law and also on the efficiency of cybercrime wing of FIA to properly prove the crimes on the accused, this itself is easily a complete separate debate. The statistics do show an increase in the number of enquires launched, which means that more cases each consecutive year were reported and then later inquiries were launched against the complaints. The current procedure of registering an FIR on cybercrime follows more of an online approach rather than the traditional approach of visiting the police station and manually registering the FIR. This online approach is much more efficient since the reporter does not need to go anywhere and can simply register the complaint from the comfort of their homes, the other benefit is that the online complaint is registered immediately and officers from FIA are bound to do some proceeding on the matter. The downside of this automated system is that often people are not sure if something as an online FIR of cybercrime exists and most do not understand on how to use the system, we have a vast majority of people who are using social media and internet services but are not literate enough to write things in detail and use sensitive reporting systems. Another issue which occurs is the prank complaints registered on the system, although legal action can be taken against the pranksters but the system does end up being filled with spam.

Overall it is very safe to say that cybercrime laws are not being utilized even half of what should be expected, it is mostly due to unawareness and illiteracy of the general public, another issue that is often experienced is that mostly people are not aware of their activities that are actually criminal under the cybercrime laws. It can be safely assumed that both the public and FIA as the governing body on cybercrimes need to bridge up the gap between each other so that more crimes are reported and the law is implemented properly and efficiently.

DEVELOPMENT OF CYBERCRIME LAW IN PAKISTAN

In Pakistan, cybercrime wasn't taken seriously until recently as there was no awareness regarding it. There was no specialized law concerning cybercrime some years back, but then again the rampant and phenomenal increase in cybercrime is fairly new and can be traced back to the past few years thus emphasizing the need for special cybercrime legislation.

In 2002, Electronic Transactions Ordinance was passed which was the first IT relevant legislation created by lawmakers. It provided for electronic documentation and authentication. There was no accreditation or recognition for electronic documents before the passing of ETO. Cybercrime was also recognized in ETO wherein unauthorized access and damage to information system were made punishable. This law though serving as a starter and a building block for other laws to come was lacking and did not cover many means of cybercrime. The questions that have recently appeared due to growing use of digital media called for formation and execution of separate legal framework and the need for specialized cybercrime legislation was felt even more which could guard the "digital rights" of individuals.

The deliberations on new cybercrime legislation began in 2014 after the APS attack where terrorists attacked an elementary school in Peshawar and murdered nearly 150 students and teachers. The APS incident presented a novel situation in Pakistan and shortly after the attack, Pakistan created a "National Action Plan" consisting of 20 action items the country would implement to counter extremism. In February 2015, a draft bill was approved to be introduced to the parliament. The bill was approved by the National Assembly in April 2016. The Senate unanimously passed the bill in July 2016 with 50 amendments to the original draft. The amendments were sent back for debate to the National Assembly, which passed the bill in August. The same month the President assented to the Prevention of Electronic

Crimes Act (PECA) 2016, bringing the anti-cybercrime legislation into effect.

PECA recognises hacking, identity theft, cyberbullying, cyberstalking, digital piracy, spoofing, doctoring images as serious punishable offences. It also recognises electronic fraud, forgery, unauthorised access into an information system as serious offences. Moreover, the Prevention of Electronic Crimes Act (PECA) of 2016 grants punishment of sentences in jail and fines also.

This act was a hasty attempt to curb the evils such as cybercrime, terrorism, violence, hate speech by digital means and to counter constantly increasing crimes originating from digital spaces. The rationale for the legislation, as presented by the then-Minister of State for Information Technology, was that existing laws were inadequate to deal with new, unprecedented, and unique types of cybercrime, such as hacking, cyber terrorism, and identity theft, among other offences. It was claimed that PECA would protect citizens from cyber threats, prevent cybercrimes, contribute to national security, and enable a secure environment for the Information Technology industry. These claims were fiercely contested by civil society representatives who highlighted the human rights concerns about the bill during the rushed legislative process.

IV. PECA: A CRITICAL ANALYSIS

PECA aims at countering all crimes by digital means. PECA is a penal law and has strict penalties and punishments whereby cybercrimes such as hacking, cyberstalking, spoofing, unauthorised access of information systems, etc., are made punishable. It is, however, a very poorly drafted law.

Any law which is penal in nature and does put criminal liability on the subjects must be very clear and accurate. However, throughout

the act, there are ambiguities surrounding its provisions. Section 3 of the act, for instance, makes punishable a person who 'with a deceitful and dishonest intention' gains access to any data or information system without having authority to do so. Now, the problem here is that there no yardstick provided in the law to judge the degree of dishonesty. There is nothing in the Act that explains what a dishonest intention is or what will be deemed dishonest. Moreover, it raises another question, i.e., if the dishonest intention is punishable, what about the person who proves an absence of dishonest intention and deceit on his part? Does that justify his accessing or violating the personal data of another person?

There is a "void for vagueness" doctrine regarding the law carrying vague terms. Law, especially a penal law, must define the criminal offence with enough definitiveness and in clear terminologies. It must be such that a common person can easily understand and can have the knowledge about the prohibited conduct. It must not leave people guessing at what it would mean and what the offence would consist of.

In *Conally v General Construction and co*[25], the US Supreme Court ruled that law is unconstitutionally vague when "people of common intelligence must necessarily guess at its meaning."

A number of provisions in the act can be rendered void on these grounds being vague and ambiguous as they are violative of the right of fair trial and due process of law as provided for in Article 10-A of the constitution of Pakistan. Due process of law involves that a person knows what offence is he being charged with and what act or series of acts he committed that constitutes the offence he is being charged with.

PECA is also criticised on the grounds that it gives vast and discretionary powers to authorities which are again violative of due process of law, opening doors for abuse of the law. To give an

[25] *Connally v. General Construction Co.* (1926) 269 U.S. 385.

example, the standard by which dishonesty of the intention of the offender, which is an ingredient of a number of crimes in this act, is measured is entirely at the discretion of the authority. Similarly, there is no standard to measure the "intent for wrongful gain," "intent to cause damage and injury," and the judgment is left to the arbitrary whims of the authority, thereby giving unbridled and unfettered powers to the authority which is Pakistan Telecommunication Authority as defined in PECA.

In the Prevention of Electronic Crimes Act, the term "cyberterrorism" is too broadly defined as the commission of any crime that falls under section 6 to 9 of the act "with the intent to coerce, intimidate, overawe or create a sense of fear, panic or insecurity… in public". This definition can be easily misapplied, and many non-terrorism cases can be conveniently brought in this category in the executive discretion and given a much harsher punishment, especially as is seen, that historically it has already been done and terrorism laws have been misapplied a lot in the past.

The Reprieve and Justice Project Pakistan ("Justice Project"), a non-profit organisation that analyses Pakistan's prison system, in a study concluded that 80% of prisoners convicted of “terrorist offences” had nothing to do with terrorism. Only 20% were genuinely terrorists, as the word is commonly understood.[26]

This act divides the offences provided in the act into cognisable and non-cognisable offences. Only three cyber offences in the PECA have been declared cognisable offences, and all others are non-cognisable offences. The offences of cyber terrorism, child pornography, and the use of sexual images online for blackmailing purposes are cognisable offences under PECA. Cognisable offences are those offences in which the investigators don't have to seek a

[26] Justice Project Pakistan and Reprieve, ‘Terror on Death Row: The Abuse and Overuse of Pakistan’s Anti-Terrorism Legislation’ (December 2014) (Terror on Death Row Report).

warrant from a court, and they can arrest for investigation without a warrant.

Section 30 is the provision in the act providing for a search warrant by the court on the application of investigating officer. It uses the word "may," thus giving out a permissive language. Section 31 again uses the word "may" for allowing the warrant for disclosure of data to order a person to turn over data. These provisions look too convenient and give out the impression that the judge can easily not allow the warrant for further investigation if he is not satisfied. These provisions impede the investigation in cybercrime cases as for an investigation into an online crime, the prior permission of the court is necessary. This has been pointed out by the Director Cyber Crime Wing (CCW) of FIA Waqar Ahmed Chauhan on a recent occasion. Already with the lack of capacity and resources, FIA cannot sufficiently investigate complaints. This condition of prior permission by the court presents a further hindrance.

On the other hand, it is seen that though the offences in PECA are non-cognisable, meaning thereby FIA cannot act on its own to investigate crimes under the act, in practice, a swift glance at FIRs has shown that the cognisable sections of PECA, Penal Code and Terrorism laws have been routinely added to gain powers to make an arrest and start inquiry. This practice by authorities is a misuse of law, and instead of adopting this course, the law must be amended to give the authorities the required power to deal with the cases in its domain.

Another major loophole in PECA is that it does not adequately address the problem of lack of jurisdiction over global Internet companies when it comes to content regulation.

It is worth mentioning that Pakistan does not have a separate data protection law. When dealing with the question of safe cyberspace, data protection is a moot point. In Pakistan, PECA acts as the only legislation in terms of data protection. However, it does not deal with the subject of data protection effectively but to a very limited extent.

Legislature did come up with a separate Data Protection Act formed on the lines of GDPR, which is hailed as the "gold standard" for data protection laws. The Act, unfortunately, has not been passed and is still in the bill stage. So, for now, PECA is the regulatory legislation on the subject of data protection. But PECA leaves loopholes here too.

PECA allows real-time data collection with a court warrant, but this is extremely problematic as this legal provision can be used to set up an invasive surveillance technology that could be used to selectively or broadly monitor citizens. The section is also in contradiction of the real-time surveillance procedure defined in the Fair Trial Act.

PECA also allows Internet Service Providers to retain traffic data for a whole year and give access to PTA if required by it during any investigation. This one-year time duration is far more increased now than the previously allowed duration of 90 days. And this retention of traffic data is again violative of privacy according to international standards. The act does not define protocols of how the retained data is to be stored, and this way puts citizens' data at risk of breach. Without special data protection and privacy law, the retention of traffic data poses concerns for the privacy of citizens as the data could be misused, for example, surveillance or targeting of individuals.

In these recent years, Pakistan has seen a rise in child pornography cases. Under section 19(3), any person who "produces, offers or makes available, distributes or transmits through an information system or procures for himself or for another person or intentionally possesses material" depicting a minor engaged in sexually explicit conduct is punishable with imprisonment up to seven years or fine up to 5 million rupees or both.

However, case studies have shown that people who engage in such crimes usually belong to a pornographic ring.[27] One of the aims of sentencing is to provide a deterrent for the masses. And individual punishment to a single felon when such pornography-producing mafia is on the rise does not serve the purpose. Therefore, a provision providing for a severer punishment for these kinds of groups should be introduced in the law.

Another prevalent cybercrime in Pakistan is online harassment and blackmail, usually done by posting compromised pictures and videos of the victim online. These crimes are made punishable under section 21 of the Act and provide for a punishment of imprisonment up to one year or fine up to one million rupees or both.

Cyber harassment and blackmail are very traumatic for the victim and take a huge psychological toll on the victim. One case is that of the Sindh University student, Naila Rind, who committed suicide after being blackmailed and harassed.[28] This is not just one case; the numbers of such cases of harassment have only increased. According to the Digital Rights Foundation, it received 2,023 complaints to its Cyber Harassment Helpline in 2019, "accounting for 45% of the overall complaints received in the last three years," with 58% of the grievances being from women. In its report, it revealed that 40% of women in Pakistan had experienced some kind of harassment on social media sites.[29]

The facts beg the question of why abuse, harassment, and trolling online are becoming normal and prevalent. One reason is that the laws

---

[27] 'Man Convicted under Cybercrime Law for Child Pornography' *Digital Rights Foundation* (June 20, 2018) <https://digitalrightsfoundation.pk/man-convicted-under-cybercrime-law-for-child-pornography/> accessed 19 April 2021.

[28] Khan MH, 'Sindh University Student Naila Rind Committed Suicide after Exploitation, Blackmail Police' *The Dawn* (December 4, 2017) <https://www.dawn.com/news/1374502> accessed 19 April 2021.

[29] Bukhari A, 'Silent Battles: How Pakistani Women Counter Harassment in Cyberspace' *The Diplomat* (October 21, 2020) <https://thediplomat.com/2020/10/silent-battles-how-pakistani-women-counter-harassment-in-cyberspace/> accessed 19 April 2021.

safeguarding from such harassment are not implemented effectively. No matter how detailed the law is, if it is not implemented in an effective manner, it is merely an addition in the law library.

Another major reason why cyber harassment is increasing is that people think they can get away with anything online. It gives them a mask behind which they can hide. People also have a negative concept of freedom of speech in their minds. Especially in the case of online trolling, people try to justify it in the name of freedom of speech. But in reality, freedom of speech is not an absolute right and carries with itself duties and responsibilities. Therefore it is subject to restrictions provided by law. For example, Article 19(3) of the ICCPR imposes restrictions on the following grounds:

(a) For respect of the rights of reputations of others
(b) For the protection of national security, or public order, or public health or morals.

FREEDOM OF EXPRESSION IN LIGHT OF PECA

All laws and regulations in a state are eventually passed for the protection and promotion of rights and safeguards of individuals and any law which has the effect of taking away and restraining constitutional rights of individuals is against the letter and spirit of law. Prevention of Electronic Crimes Act has faced a lot of backlash since its promulgation from civil society for violating fundamental right of speech which is provided for in Article 19 in the constitution. Freedom of expression and speech are the cornerstones of democratic society. Criminalizing peaceful expression is a step in the backward direction for the country.

The Pakistani Constitution of 1973 maintains the essentials for a vivacious democracy and pledges freedom of expression (Khalid Aziz vs. Pakistan Television Through Managing Director).[30] Freedom

[30] Khalid Aziz v. Pakistan Television (2017) PLD Peshawar 115.

of speech was defined by the Lahore High Court as "an expression or communication of thoughts or opinions in spoken words. An expression of or the ability to express thoughts and feelings by articulating sounds or a sequence of lines written for one character in a play". Whereas freedom of expression means "the action of making known one's thought or feelings; the conveying of feelings in a work of art or in performance of a piece of music; writings, speech, or action that show a person's ideas, thoughts, emotions or opinions. Expression include speech. Any dramatic work is therefore a symbol of speech and expression. The right to communicate and receive ideas, knowledge, information, beliefs, theories, creative and emotive impulses by speech or by written words, theatre, dance, music film, through a newspaper, magazine drama or book is an essential component or the protected right of freedom of expression (Leo communications Limited vs. Federation of Pakistan, 2017)[31]

PECA has been severly criticized for violating and threatening the important rights and liberties of the individuals namely right to freedom of expression and speech as provided for in Article 19 of the constitution of Pakistan. However, a 'Bare examination of Article 19 of Constitution presents it clearly that this right of freedom of expression is not unqualified but a limited right. Limitations on freedom of expression may be levied if it meets the necessities of "reasonableness". Nevertheless, the word "reasonableness" is not well-defined in the Constitution. It is neither conceivable nor advisable to present any theoretic standard of general application of reasonableness'[32]

The superior Courts has defined this reasonableness and prescribes that "when state wishes to deny to its citizens the

[31] Leo Communication (Pvt) Ltd vs. Federation of Pakistan (2017) PLD Lahore709.
[32] Fazeel Ahmer, *The Constitution of the Islamic Republic of Pakistan* (Karachi: Pakistan Law House, 2002).

enjoyment of fundamental rights enshrined under the constitution; three significant features must be accomplished"[33]

a) The restrictions on expression under article 19 can only be levied by the authority of law, no restriction can be levied by the authority of executive of the country.

b) Each restriction must fulfill the condition of reasonable restriction.

c) Restriction should be allied to the objects declared in Article 19[34]

Article 19 grants the power to parliament to enforce "reasonable restrictions" on freedom of expression in the "Interests of or in the Glory of Islam, Integrity and Security of State of Pakistan, Friendly relations of State with foreign states, public order, decency or morality, contempt of court and defamation." To decide and determine what these reasonable restrictions will be and how will they be imposed is the job of the parliament. These are to be legislated upon by the parliament. However, interpretation of law being a judicial function, the judicial authorities can interpret these "reasonable restrictions" laid down by parliament. Essentially speaking, the power to decide what these restrictions would be a combination of legislature and judiciary's work, and the executive cannot in any circumstance be given that kind of power. But PECA provides unhinged powers to PTA to curtail the fundamental right of speech. And for this reason PECA is so widely hailed as a black law because it gives too much power to executive authorities to limit freedom of speech in Pakistan.

---

[33] Srivastava, Romit, 'Test to Determine Reasonable Restrictions Under Article 19 of the Constitution of India' (August 24, 2012) <http://dx.doi.org/10.2139/ssrn.2135681 > last accessed 15 March 2021.

[34] Muhammad Ashraf et al., "The Prevention Of Electronic Crimes Act 2016 And Shrinking Space For Online Expression In Pakistan" (2020) 43 Hamdard Islamicus: quarterly journal of the Hamdard National Foundation, Pakistan 231-242.

A number of provisions in PECA have the effect of curtailing freedom of speech and expression of individuals in Pakistan. This law being so arbitrarily and vaguely worded can be used by the political elite and other authorities to stifle the voice of an ordinary man. And keeping history into account, it is being used for this purpose arbitrarily by the authority.

PECA criminalises free speech without providing sufficient safeguards and minimising the room for satire or political criticism or expression[35] by individuals and that too on the whims of the authority. Section 18 of the Act makes punishable any person who "displays or transmits any information which he knows to be false" This section has a far-reaching effect as it applies to everything shared online.

This section can be extremely misused and misapplied. To give an example, in 2016, the Turkish court sentenced a man named Cetin to one year in prison on the grounds that he had shared and compared pictures of prime minister Erdogan and Gollum (a character from the Lords of the Rings Trilogy) on Facebook.[36] Will the same consequence ensue if someone compared a picture of any Pakistani politician to any fictional figure? Will the punishment be justified? Will it not limit even the most harmless and innocent expression, which is the basic fundamental right of every individual? This section will restrain every kind of satire, political expression and will have the effect of silencing people on their political views; otherwise, they will be sentenced to jail.

PECA is notorious for its "over regulation" of online content and giving vast powers to authority to block content. Section 37 of the Act gives PTA the power to remove and block online content if it is against the glory of Islam, defence of country and public order,

---

[35] 'Major contentions: PECA' <http://bolobhi.org/wp-content/uploads/2016/10/Majorcontentions-PECA-201> (Bolo Bhi 2016) last accessed 16 March 2021.

[36] 'Turkey guilty verdict for depicting Erdogan as Gollum' *BBC* (23 June 2016) <https://www.bbc.com/news/world-europe-36610000> accessed 17 March 2021.

morality etc. Again these considerations are too subjective and too broad. It gives the authority unhinged power to limit the expression of people as to its own liking. There is no yardstick to see what acts are deemed to be against the defence of country, or public policy, or morality, etc. This is totally left to the subjective judgement of the authority. Whatever the authority thinks is against these considerations, it can act unilaterally to block and remove that.

If the right of free speech and expression is to be constrained, it must have some reasonable constraints which only a court of law can provide for. PTA should not have the power to do so. It is a fundamental right and needs to be safeguarded. That is the duty of the state.

In the past we have seen that PTA has exercised this discretion quite unreasonably blocking numerous websites and content. Sometimes in the name of preventing blasphemy and sometimes in the name of anti state statements. This regime of self-censorship started by PTA has very badly affected the country's reputation. A study conducted by the Digital Rights Foundation confirmed that the detection of 210 blocked URLs in Pakistan under section 37 of PECA. Up until 2019, PTA blocked 900,000 web pages on the grounds that they were blasphemous, pornographic, unsuitable, or inappropriate. These statistics were revealed by the PTA officials themselves.[37] There were, however, no details released as to what considerations were weighed in such decision making or the names of the web pages that were blocked[38]

While the basic purpose of the Prevention of Electronic Crimes Act is to counter digital crimes, but unfortunately, most of the

---

[37] Ali K, '900,000 Websites Blocked over Content, Says PTA' *The Dawn (*September 2019) <https://www.dawn.com/news/1507590> accessed 15 March 2021.

[38] Jahangir R, 'PTA's Content Removal Conundrum' *The Dawn* (July 27, 2019) <https://www.dawn.com/news/1496491> accessed 15 March 2021.

provisions have the objective and effect of blocking free speech and expression.

RECOMMENDATIONS & CONCLUSION

Despite the promulgation of acts to combat cybercrime, lawyers and rights activists lament that implementation has been slow and insufficient. The issue of the increase in cybercrime and the loopholes in PECA have been discussed in detail in the previous sections of this paper. This paper is an attempt to make PECA more practical and implementable for the people of Pakistan in the hope that the competent authorities would recognise the highlighted issues and adopt the following recommendations/implementation guidelines:

1. A thorough and complete review of PECA 2016 needs to be conducted. The review must address the contradicting legal sections and the practical implementation problems as well. The review must be conducted by all stakeholders of the society, including legal experts, civil society representatives, and most importantly, technical experts. The inclusion of technical experts is of paramount importance since PECA 2016 addresses a technical crime involving the use of technology.

2. All efforts must be made by the government to review sections of the law that are in violation of the fundamental rights of individuals, and amendments and revision of the sections must be made. Affirmative legislation that protects and promotes speech, privacy, and data must be introduced.

3. The Government should start the amendment process in PECA 2016 and should try to make the Act more public-friendly and focused on public benefits. Currently, PECA ensures stricter action on certain sections than it should.

4. The merger of content regulation into cyber offences in PECA should be treated as separate concepts. A separate 'digital content moderation' or 'digital content regulation' framework should be made in order to ensure the protection of freedom of expression as a fundamental right.

5. Section 37, which allows PTA to block online content, should be revised urgently to define the parameters and conditions for removal in a more transparent manner. It would be best if this section is removed from PECA and be placed in the new suggested framework in point three.

6. The State should focus on empowering the officers dealing with cybercrimes. FIA officers should be given technical training as per international standards. There is a great need to build up the technical capacity in FIA to address these ever-changing nature of cybercrimes. There is also a need to build up a judicial capacity for such cases, and there should be a technical judicial advisory council tasked with ensuring the honourable judges have a better understanding of the nature of cybercrime.

7. A separate judicial cell should be established to hear these cases, as our courts are more occupied with other criminal proceedings.

8. There is a dire need to launch a public awareness campaign to help the public understand the existing cybercrime laws and their reporting. FIA and PTA should start launching public service messages on media platforms so that more and more people get educated about cybercrimes. FIA and PTA should publically make clear their domains and establish the types of cases that they will be managing.

9. FIA should launch 24/7 call centres or even physical care centres for the public to provide adequate guidance and proper feedback on their complaints. The FIA reporting portal should be made more user-friendly, and more facilitation measures should be

placed online, such as online chat or call as well. FIA needs more skilled human resources to manage cybercrimes effectively, and nationwide cyber forensic labs should be established.

It must be understood that revising PECA cannot be a revolutionary process, and rather it is an evolutionary process. In light of the discussion highlighted in this paper, it can be seen that cybercrimes are prevalent in our society, and they have been ignored for a very long period. PECA 2016 served as the building block of proper cybercrime legislation in the country. The long-lasting issues with PECA are its contradictions with existing articles of the constitution and its lack of proper implementation guidelines. It has been observed that in the past, some laws were abused to facilitate the criminals instead of apprehending them. Laws should be made in order to maintain public order and to keep harmony among the society. The main aim should always be the benefit of the entire public, ensuring their fundamental rights. The recommendations discussed above are needed to make PECA more practical and implementable for the general public; the state always wants to help and empower its people and making the required changes in PECA 2016 would help build more trust among the people and would also slow down the sharp rise in cybercrimes

BIBLIOGRAPHY

Primary Sources

Case Law

1. Connally v. General Construction Co. (1926) 269 U.S. 385
2. Khalid Aziz v. Pakistan Television (2017) PLD Peshawar 115
3. Leo Communication (Pvt) Ltd v Federation of Pakistan (2017) PLD Lahore 709

Secondary Sources

Books and Articles

10. *'A Short History of the Web' (CERN) <https://home.cern/science/computing/birth-web/short-history-web > accessed 19 April 2021*
11. 'Major contentions: PECA' (Bolo Bhi 2016) <http://bolobhi.org/wp-content/uploads/2016/10/Majorcontentions-PECA-201> last accessed 16 March 2021
12. 'Man Convicted under Cybercrime Law for Child Pornography' *Digital Rights Foundation* (20 June 2018) <https://digitalrightsfoundation.pk/man-convicted-under-cybercrime-law-for-child-pornography/> accessed 19 April 2021
13. 'What Is a Denial-of-Service (DoS) Attack?' (Cloudflare) <https://www.cloudflare.com/en-gb/learning/ddos/glossary/denial-of-service/> accessed 2 May 2021
14. 'What Is Phishing?' (*Phishing.org*) < https://www.phishing.org/what-is-phishing#:~:text=Phishing%20is%20a%20cybercrime%20in,

credit%20card%20details%2C%20and%20passwords > accessed May 2, 2021

9 A Ahmed and DS Khan, "Cyber Security Issues and Ethical Hacking in Pakistan" (2015) Department of Computer Science Karachi University

15. Ali K, '900,000 Websites Blocked over Content, Says PTA' *The Dawn* (27 September 2019) <https://www.dawn.com/news/1507590> accessed 15 March 2021

16. Allia Bukhari, 'Silent Battles: How Pakistani Women Counter Harassment in Cyberspace' *The Diplomat* (21 October 2020) <https://thediplomat.com/2020/10/silent-battles-how-pakistani-women-counter-harassment-in-cyberspace> accessed 17 March 2021

4. DH Jaishankar, *Cyber Crime and the Victimisation of Women: Laws, Rights and Regulations* (Hershey, PA: Information Science Reference 2012)

5. Fazeel Ahmer, *The Constitution of the Islamic Republic of Pakistan* (Karachi: Pakistan Law House 2002)

17. Federal Investigation Agency <http://fia.gov.pk/en/NR3C.php> accessed 2 May 2021

18. Forcepoint. (n.d.). 'What is Spoofing?' < https://www.forcepoint.com/cyber-edu/spoofing> last accessed 17 March 2021

19. Jason R. Ingram, "Digital piracy" (2014) The Encyclopedia of Criminology and Criminal Justice

20. Justice Project Pakistan and Reprieve, 'Terror on Death Row: The Abuse and Overuse of Pakistan's Anti-Terrorism Legislation' (December 2014) (Terror on Death Row Report)

6. Majid Yar, *Cyber Crime and Society* (London: SAGE Publications Ltd, 2006)

21. Marc D Goodman and Susan W Brenner, "The Emerging Consensus on Criminal Conduct in Cyberspace" (2002) Int J Law Info Tech 10 (2): 139

22. Marc D. Goodman, "Why the Police Don't Care About Computer Crime" (1997) 10 HARVARD J. LAW & TECH. 465, 468–469
23. Mark M. Pollitt, '*Cyberterrorism—Fact or Fancy?*', Proceedings of the 20th National Information Systems Security Conference, 285, October 1997 (quoted in Dorothy E. Denning, *Activism, Hacktivism and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*, <http://www.nautilus.org/info-policy/workshop/papers/denning.htm> accessed 17 March 2021
24. MH Khan, 'Sindh University Student Naila Rind Committed Suicide after Exploitation, Blackmail' *The Dawn* (4 December 2017) <https://www.dawn.com/news/1374502> accessed 19 April 2021
25. Muhammad Ashraf et al., "The Prevention Of Electronic Crimes Act 2016 And Shrinking Space For Online Expression In Pakistan" (2020) 43 Hamdard Islamicus: quarterly journal of the Hamdard National Foundation, Pakistan 231-242
26. National Response Centre for Cyber Crime <http://www.nr3c.gov.pk/> accessed 2 May 2021
7. Prashant Mali, *A Text-Book of Cybercrime and Penalties* (Indiana: Repressed Publishing LLC, 2006)
27. R Jahangir, 'PTA's Content Removal Conundrum' *The Dawn* (27 July 2019) <https://www.dawn.com/news/1496491> accessed 15 March 2021
28. Rizwan Shehzad, 'Only 14 cybercrime convictions in five years' *Tribune Pk* (20 July 2020) <https://tribune.com.pk/story/2255771/only-14-cyber-crime-convictions-in-five-years> accessed 17 March 2021
8. S Furnell, *Cyber Crime: Vandalising the Information Society* (London: Addison Wesley, 2002)
29. Shakeel Qarar, 'Cybercrime reports hit a record high in 2018: FIA' *Dawn* (23 October 2018) <https://www.dawn.com/news/1440854> (accessed 16 March 2021)

30. Shakeel Qarar, 'FIA arrests man accused of obtaining, distributing child pornography on social media' *Dawn News* (29 December 2020) <https://www.dawn.com/news/1598523/fia-arrests-man-accused-of-obtaining-distributing-child-pornography-on-social-media > accessed 17 March 2021
31. Simon kemp, 'DIGITAL 2021: PAKISTAN' *DataReportal* (11 February 2021) <https://datareportal.com/reports/digital-2021-pakistan> accessed 17 March 2021
32. Srivastava, Romit, 'Test to Determine Reasonable Restrictions Under Article 19 of the Constitution of India' (24 August 2012) <http://dx.doi.org/10.2139/ssrn.2135681> accessed 17 April 2021
33. T Kumar et aal., "Cyber Crime And Their Solution"(2012) 1 International Journal Of Engineering And Computer Science, 48-52
34. Talha Khan, 'Cybercrimes: Pakistan lacks facilities to trace hackers' *Express Tribune* (01 February 2015) <https://tribune.com.pk/story/831178/cybercrimes-pakistan-lacks-facilities-to-trace-hackers> accessed 17 March 2021
35. 'Turkey guilty verdict for depicting Erdogan as Gollum' *BBC* (23 June 2016) <https://www.bbc.com/news/world-europe-36610000> accessed 17 March 2021