AL-HAYAT Research Journal
Jlali Research Institute of Social Science, Lahore
Category Y
ISSN (Online): 3006-4767
ISSN (Print):: 3006-4759
Volume 2 Issue 3 (April-June 2025)

Cyber Legislation and Cyber-Victimization in Pakistan

Aliya Saeed
PhD Fellow at School of Law, University of Karachi, Pakistan, aaliasaeed@yahoo.com

Dr. Tansif Ur Rehman
Teaching Associate, Department of Sociology, University of Karachi, Pakistan; and Visiting Faculty, Department of Law, Dadabhoy Institute of Higher Education, Pakistan (tansif@live.com) (https://orcid.org/0000-0002-5454-2150)

Dr. Adeel Abid
Advocate Supreme Court of Pakistan; and Assistant Professor, Department of Law, DIHE, Karachi, Pakistan adeel77abid@yahoo.com

Adnan Zawar
M.Phil. Research Scholar, Institute of Social & Cultural Studies, University of the Punjab, Pakistan
adnan.zawar@gmail.com

Syed Adeel Ali Bukhari
Ph.D. Research Scholar, Department of Public Administration, University of Karachi, Pakistan
adeelali84@hotmail.com

Abstract

Pakistan is experiencing an exponential use of social media. Pakistan has a high likelihood of theft of finances and hacking of accounts that conduct e-transactions and store important data on e-devices. In Pakistan, there are laws against cybercrime that are hardly enforced. In Pakistan, the respective culprits tend to escape punishment. After conducting several amendments in the Electronic Crime Bill 2016, it was passed by the National Assembly of Pakistan. Even this bill was highly opposed in Pakistan. The study evaluates and examines the current situation of cybercrime in Pakistan.

Keywords: Cyber Legislation, Cyberterrorism, Hacking, Pakistan, Cyber-Victimization

Introduction

Cybercrime is a criminal act that is perpetrated using either computers or the Internet (Collins English Dictionary, 2020). According to the Chambers Dictionary (2020), it is a criminal activity or a crime that involves the Internet, a computer system, or computer technology, according to Encyclopedia Britannica (2020), cybercrime, a computer as a tool to pursue criminal acts, such as perpetrating fraud, exchanging child pornography and intellectual property, stealing identities, or intruding on privacy. The computer has increased in popularity with cybercrime, more so via the Internet (Abaimov & Martellini, 2020; Johansen, 2020; Lavorgna, 2020; Littler & Lee, 2020).

Merriam-Webster (2020) defines criminal activity (fraud, theft, or child pornography distribution) as a crime carried out through a computer, particular to gain unauthorized access to, distribute, or corrupt data. Although, according to the dictionary of Advanced Learners, Oxford (2020), the committed crime must be executed via the Internet, e.g., by stealing someone's personal/bank data or by giving the person a virus. In 2007, the National Response Center of Cyber Crime (NR3C) came into being in Pakistan. Downplaying cybercrime, making it seem like it is always the deed of a single person, is sometimes tempting, but again, it is only that way in some instances, whereas the full picture of cybercrime is quite unlike that.

This research includes case studies involving violations of authenticity, confidentiality, as well as human integrity. It is discussed in different newspapers as well as TV channels in Pakistan. Their authenticity is checked through multiple reliable sources, like press releases or law enforcement agencies of Pakistan, namely the Federal Investigation Agency,

National Database, and Registration Authority, and Provincial Police Department related to the computer-crime and cybercrime division, as well as through multiple relevant and authentic websites. This paper dwells on cyber laws and cyber-victimization in Pakistan. Purposive sampling was used, which was the qualitative research methodology, and five cases were selected. It is because of that that it is explanatory in nature.

Focus of the Research

This research assesses and analyzes cybercrime's current state in the Pakistani context. The incidents with the victim's name changed are documented in this research. The following case studies were chosen because they are the most prominent cases that made headlines and are still debated across the country. Two case studies of fraud, two case studies of hacking, and a case of cyberterrorism were chosen to highlight the recent cybercrime trends in Pakistan.

Research Methodology

This paper will be devoted to cyber legislation and cyber-victimization in Pakistan. The qualitative research methodology, with the help of purposive sampling, was chosen, and five case studies were sampled.

Pakistan in the Cyberworld

Pakistan is no exception, as the abuse of technology is widespread in the country, with the rate of cybercrime rising at an alarming rate. Pakistan is also one of those nations that are confronting transnational cybercriminals as well as local threats. Pakistan is another country that has not taken the cybercrime issue lightly and has come up with a legal framework. The 2002 enactment of the Electronic Transactions Ordinance is a robust level of security of documents, information, records, communication, and transactions in electronic form, as well as assigning the official authority of certification to the Internet Service Providers (ISPs). The concerned framework has now accorded Pakistan with legal support on e-information as well as communication.

Over 30 million out of Pakistan's (212 million) population access the Internet through their mobile phones. Cybercrime in Pakistan is getting out of proportion. It is a rapid arising felony that is even difficult to detect. In Pakistan, the cybercrime cell gets approximately 12 complaints each day. Strong programs must be implemented in such a way that people are not afraid of being infected in the process of browsing the web.

Electronic Transactions Ordinance, 2002

The adoption of the Electronic Transactions Ordinance, 2002 (ETO) has ensured that Pakistan is among one of the few nations that realized the significance of cybercrime law in the early days and offered urgent guidelines and frameworks that facilitated and promoted the IT industry to rise to higher heights and spread e-commerce in Pakistan. The Electronic Transactions Ordinance is crucial in the execution of the appropriate IT development and is regarded as a breakthrough in Information and Communication Technology development and growth in Pakistan.

National Response Center of Cybercrime

Another effort made by the Government of Pakistan in order to trace cybercriminals as well as counter internet abuse is the establishment of the National Response Center for Cyber Crime (NR3C) in 2007. With respect to the Certificate Authority (C.A.), the accreditation was established as the Accreditation Council under the National IT Policy and Electronic Transactions Ordinance, 2002, by the Ministry of Information Technology and Telecommunication. The programs of this voluntary licensing are geared towards having a high integrity of licensed C.A.s who can be trusted. A Certificate Authority seeking to obtain a license will use more rigid licensing criteria, which will comprise:

1. Stringent security measures and controls.
2. Personnel integrity
3. Financial soundness

Critical Analysis of Pakistan's Cyber Legislation

The trend and the impact of the Internet are definitely a good omen in any society. At the same time, it is also a risk to a nation such as Pakistan. Despite the fact that IT is becoming an indispensable part of our daily lives, the other side is rather threatening. The literature rate of the country is comparatively low according to the Economic Survey of Pakistan 2017; in other words, it is 58 percent. Even in the context of Information Technology education and awareness, it is horrific and even alarming in the Pakistani context. Therefore, it presents a treasure trove of vulnerability to cybercriminals to take advantage of. The Prevention of Electronic Crimes Act, 2016, can be described as a brilliant success of the legislative parliament of Pakistan to prevent cybercrime and streamline ICTs.

With the availability of ICTs and global connectivity in Pakistan, the tendency to accelerate and increase the rate of cybercrime activities has been realized globally. The explanation is very self-evident because they no longer need to be physically present in the crime they want to commit. Digital crimes that are easier to execute with the help of the Internet, speed, convenience, anonymity, and worldwide presence include financial crimes, such as ransomware, fraud, and money laundering, hate crimes, such as stalking and bullying.

Cybercriminals steal and sell private information and corporate data in the cybercriminal black markets that have multiplied several-fold in cyberspace (Austin, 2020; Bandler & Merzon, 2020; Marion & Twede, 2020; Troia, 2020). Any effort to steal financial accounts, credit cards, or other payment cards is one of the largest threats to the economic organization of Pakistan. John Carlin (1997) said that the possibility of insecurity accompanies the convenience of digital connectivity. Prevention of Electronic Crimes Act, 2016, is a very much needed measure that is being taken in the right direction. It provides the safety of the IT consumers and encompasses the greatest scope of crime that could be perpetrated by the criminals against society, people in a group, corporate entities, institutional establishments, and individuals. These offenses can result in psychological suffering and economic disillusionment, disrupting or weakening the state institutions or other organizations via the technology of ICTs and networks.

On 13 April 2016, the draft of the Prevention of Electronic Crimes Act, 2016 (PECA) was passed by the National Assembly of Pakistan. A legal framework against a computer attack was one of the major reasons that led to the drafting of the corresponding Act. This Act had provisions by enlisting in Sections 3 to 8 of the Act.

1. Unauthorized access to Information System (I.S.).
2. The illegal transfer or duplication of information.
3. Disruption of information or Data system (I.S.).
4. Hack into data or Critical Infrastructure Information System (CIIS).
5. Critical Infrastructure Data (CID) Transmission/copying without authorization.
6. Hacking of Data or Critical Information System (CIS).

Case Study 1 - ATM Fraud

A sudden, overpowering fright spread among the Pakistan people when the news was broken regarding Automated Teller Machine (ATM) skimming fraud. The culprits collected information, like ATM card numbers and PIN codes, by installing skimming devices in ATMs throughout Pakistan, especially Karachi. Criminals used personal information to withdraw cash in China and a few other countries (Geo News, 2017). The Federal Investigation Agency (FIA) spoke about the matter and confirmed the theft of data and money of around 579 ATM card users in December 2017. Criminals installed the skimming devices along with hidden cameras in ATMs. Their respective banks informed account holders who were unaware of this theft, the agency shared (Geo News, 2017).

Habib Bank Pvt. Ltd., one of the targeted banks, also confirmed the theft and installation of skimming devices on four of its ATMs. Criminals installed three devices in Islamabad in different places and one in Karachi. FIA has started the investigation under the Prevention of Electronic Crimes Act. The involvement of transnational criminals from China has been identified in the inquiry. The matter has been discussed on a diplomatic level between Pakistan and Chinese officials. FIA has shared the fraud's details and evidence with the respective Chinese authorities (Geo News, 2017). The placing of skimming devices needs skills as well as expertise. It is usually used to gather the debit card user's personal information, including the debit card number and personal identification number (PIN). Criminals placed the fraudulent card reading devices that look the same as the original on ATMs and the keypad, and a hidden camera that provides them with the detailed log.

The offenders used to install the card reader on ATMs so that the card information could be recorded, and the use of a camera helped them note down the PIN code type by the customers for withdrawing cash. After recording the activities for a few days, they reconciled the data and withdrew the money from other countries. Devices were placed in crowded shopping centers in the city, like Karachi. It was also revealed during the investigation that fraudsters made other ATMs dysfunctional in the arena, so more people used the tampered one. It ultimately provided them with the maximum number of people's ATM card information. This sort of cybercrime is not new in its type. According to a Group-IB report, cybercriminals had earned more than £10.5 million by hacking ATM cards' information worldwide. It is estimated that offenders have already withdrawn around $2.6 million from other parts of the world by this technology's fraudulent use (Cuthbertson, 2018).

The sales of the respective ATM cards and credit cards take place mostly on the dark web. According to Group-IB findings, it is rare to find ATM card sales on the dark web from Pakistan. That is why this is the only reported sales of cards in the last six months (Cuthbertson, 2018). In an exclusive TV interview with Dawn News, Mr. Shoaib commented that the bank should take this scam. They should have preventive measures to ensure the security of their customers' data. The hackers have defrauded a tremendous amount from cardholders' accounts. He further said that this event indicates that banks should upgrade their IT security infrastructure and go beyond strategically to prevent future attacks (Zaidi, 2015).

The State Bank of Pakistan has noticed and advised all banks to review their security policies to prevent future thefts. It denied its operations being affected by any of the cyber attacks. It is reported that in response to this scam, around six banks have temporarily barred the international use of debit cards. This news is further endorsed by the chief

spokesperson for the State Bank of Pakistan, Mr. Abid Qamar, as he stated that, "It has come to their notice that a few banks have suspended the use of cards all over the world except Pakistan" (Geo News, 2017).

Case Study 2 - Hacking Government Websites

Pakistan is also among the affected countries of cyberattacks. Black hat hackers have targeted multiple websites. Even an army-operated site was attacked, called a DDoS attack by the international hackers, as a demo during a live interview on a radio channel. The group of hackers known as New World Hackers attacked Pakistan's Frontier Constabulary website on 10 January 2016, while a live interview on Anon U.K. Radio was in process. It happened just a few days after the wave of continuous attacks on the official government site (Cuthbertson, 2016).

It is estimated that they have attacked almost 60% of the government's official websites. In a hacker group statement, New World Hackers said that it was not a direct attack from them, but they facilitated Indian hackers, as they were asked to support. The group operates independently and still takes part in certain operations. Most of the cyber attacks on Pakistani websites are initiated from India, and it is supposed that it was in response to the Pathankot Air Force Base incident, a city in the Punjab state of India, on January 2-5, 2016, where the death of 14 people was reported. The group further explained that Indians do not attack Pakistani websites for fun, but they take it as a war. The New World Hackers said that they upgraded the capabilities of Indian hackers worldwide.

Case Study 3 - Hacking into NADRA

In 2010, the National Database and Registration Authority (NADRA) in Karachi in Pakistan, reported about a data breach. There was a break-in of computers and other equipment by thieves. Whether the contents of the stolen computers have been encrypted with disk encryption software has not been disclosed (Pakwired, 2016). There is a possibility of being linked to the main NADRA servers. The attack occurred in one of its branch offices (Shah Faisal Colony Office, Karachi). Nevertheless, the impacts of the breach are higher because the stolen computers could be linked to the central NADRA servers, enabling all the records in the country to be accessed.

Many lone hackers have managed to access Pakistani websites' vulnerabilities, as a Turkish hacker penetrated the NADRA and FIA official websites. In December 2012, a hacker named Eboz claimed to have accessed the websites by applying the simple SQL injection method, one tactic to gain a website's administrative control access (Pakwired, 2016). Various countries are also found spying on other countries' classified data present on the digital forum. In August 2014, passport data related to Pakistani citizens, which contained sensitive information and even biometric impressions, was compromised. It was a breach by the CIA and other U.S. intelligence agencies as part of their secret project named 'HYDRA' (Pakwired, 2016).

Pakistani secret agencies have even discussed their concern over the unlawful access to data servers by foreign secret services. Inter-Services Intelligence (ISI) in August 2014 censured the Israeli secret agency Mossad for its attempt to hack sensitive data. Countries like India and Israel have been condemned multiple times for their covert attempts by the Government of Pakistan (Pakwired, 2016).

Case Study 4 - FBI's Most Wanted Cybercriminal

In 2015, the Pakistan Federal Investigation Agency (FIA) took a person into custody in a joint effort with the FBI, USA. The arrested cyber criminal was detained in Karachi, and he was placed on the top 10 most wanted criminals by the USA's government (Zaidi, 2015). Mr. Noor Aziz Uddin unlawfully accessed the systems and deprived the victims of more than $50 million in November 2008 and April 2012. Further details on the FBI's official website revealed that he had a reward of $50,000 for his capture. U.S. authorities issued a federal warrant for his arrest in several states, like New Jersey and New York. He was charged with the Act of conspiracy to commit online fraud, identity and personal information theft, and unlawful access to computer systems (Zaidi, 2015).

He was accused and convicted of establishing an illegal telephone exchange, which caused heavy losses. The victims were unaware of the respective threats and dangers posed by individuals, organizations, and government bodies, not only in the United States but abroad. Noor, along with a companion, Farhan Arshad, unlawfully acquired access to private telephone systems. They crafted a trickery scheme generally known as 'international revenue share fraud.' They were illegally offering long-distance telephone calls at expensive rates. This scam cost the real owners a considerable sum of losses when they were billed heavily for unused services (Zaidi, 2015).

Case Study 5 - Reporter/Cyber Terrorist

Mr. Shahzeb Jillani is a Pakistani investigative reporter. He has served for Deutsche Welle as well as the BBC. He is currently engaged with Dunya News, a local Urdu news channel in Pakistan. He is accused of cyber-terrorism by violating two criminal code provisions and four articles of the PECA, 2016. The case is lodged against him by a self-proclaimed 'loyal citizen' on 6 April 2019. The plaintiff is a Supreme Court lawyer, and he said that he was offended by Mr. Jillani's comment during a television broadcast on 8 December 2017.

The chief of the RSF Asia-Pacific department, Mr. Danial Bastard, appealed, "We would like the court to drop these charges against Shahzeb Jillani as, in legal perspective, the case is absolutely inadmissible. Through the mighty

federal investigation agency, the Pakistani government is again abusing the laws with a view to silencing a journalist who has dared cross a red line by expressing criticism on some institutions. It is appalling to observe a case by case, that the Pakistani security agencies are closing in on their vice to the point of intimidating the entire media profession to censor themselves.

The case later released Jillani on bail, where he told RSF that he was very surprised by the case. He believes that the case against him is due to his recent story on missing persons, and his 24 March 2019 tweet, where he condemned the decision to honor a senior military intelligence officer who was mostly accused of political engineering in the 2018 national elections in Pakistan. The actual cause of the accusations was the build-up to such elections. RSF provided an overview of the diverse procedures through which the military establishment of Pakistani media tried to coerce the media executives to adopt its opinion and silence the journalists. Jillani also told RSF that he has not been well supported by his news channel's management. The top management has been informed of the case, yet they have not replied with a freeze. Pakistan is ranked 139th out of 180 countries in the 2018 World Press Freedom Index prepared by RSF.

Conclusion

It is not possible to know the extent of cybercrime prevalence in Pakistan. No easily available means exist to define the number of individuals who have been arrested or convicted of cybercrime in Pakistan. It is partially due to the nature of the cybercrime law in the Pakistani environment. The crimes in the cyberworld used to be thought to be hard to probe into. Every cybercrime can theoretically be indicted, but it is highly improbable that successive sentences would be given to all the respective malpractices that took place prior to the legislation. It has been seen that there is a rise in individuals in Pakistan who feel to are a victim.

Cybercrime is one of the significant problems regarding technology in Pakistan because it grows every second in a society where social networking and internet usage have become the norm. According to the National Response Center for Cyber Crime (NR3C) data set, around 20% of the cyber-related crimes are reported in Pakistan; the rest of the 80% remain unreported (Tanveer et al., 2016). The forms in which a complaint can be registered are online form, fax, written, and physical. To complain, the victim has to be inside Pakistan, or the case cannot be entertained. Differentiation in the categories of cybercrime in Pakistan is not that vivid. There is a difference between the kinds of laws made in advanced countries and those of Pakistan. Cybercrime laws in Pakistan are very complex, and even lodging a cybercrime incident is a hectic process. Pakistan is in dire need of making pertinent cyber laws. Pakistan is a developing country, but it has yet to develop cyber-norms, i.e., ethical in the Pakistani context and not. A low literacy rate, as well as a low employment rate, further adds to this dilemma.

Solutions and Recommendations

There should be the initiation of general public awareness programs, insofar as cybercrime is concerned, in Pakistan. It is achievable through the involvement of the community and CBOs, NGOs, INGOs, and cyber vigilantism. There should be the representation of expert opinions during legislation on cybercrime, such as criminologists, psychologists, sociologists, and IT professionals. Like in the earlier laws, consultations were not taken with experts. The data on cybercrime is to be kept in relation to its character and the level of its complexity. The Pakistani officials should share it with other nations. Thus, Pakistan might get lessons from the experience of other countries in the field.

The students must be sensitized about the vulnerability of the cyber world through seminars and workshops. The number of victims of cybercrime is very high, and the victims should have easy access to a victim where they can make complaints about the offenses through the Internet. On the domestic level, a special task force (i.e., cyber police) would need to be created to provide regular online checks of the public internet access facilities. Websites must be heavily censored on offensive (extremist) content, particularly on racial and religious hate. Pakistan is a highly unstable nation, and such content may result in civil unrest.

The Government of Pakistan officials should cultivate a good rapport with the private companies to provide their internet services to the best of their ability. Pakistan is supposed to ensure the legal department is furnished with the latest investigative technologies. The problem of cybercrimes should be communicated by various scholars on various forums, particularly the print media and electronic media. IT should also include criminological courses that emphasize cybercrime in its routine studies, social science studies, law studies, and business studies. E-transactions should be typed through genuine websites, and personal data (including passwords) should not be stored on common computers, as it is highly insecure.

Future Research Directions

Critical domains of future research that would involve cybercrime through stimulating qualitative, quantitative, or eclectic research may include:

1. Pakistan: Electronic freedom.
2. Reasons as to why cybercrime cases are not reported..

3. Cyberterrorism in Pakistan.
4. Combating violent extremism in Pakistan.
5. Inequity in cybercrime in Pakistan.

References

Abaimov, S., & Martellini, M. (2020). Cyber arms security in cyberspace. CRC Press.

Austin, G. (2020). National cyber emergencies: The return to civil defense. Routledge.

Bandler, J., & Merzon, A. (2020). Cybercrime investigations: A comprehensive resource for everyone. CRC Press.

Carlin, J. (1997, May). A farewell to arms. Wired. https://www.wired.com/1997/05/ffarms/

Cuthbertson, A. (2016, January 11). Hackers take down Pakistan government websites on live radio. Newsweek. https://www.newsweek.com/hackers-take-down-pakistan-government-websites-live-radio-413888

Cuthbertson, A. (2018, November 12). Stolen data from 'almost all' Pakistan banks goes on sale on the dark web. The Independent. https://www.msn.com/en-xl/asia/asia-top-stories/stolen-data-from-almost-all-pakistan-banks-goes-on-sale-on-dark-web/ar-BBPDQdU?li=BBP34wH&ocid=mailsignout

Cybercrime. (2020). In Collins English Dictionary. https://www.collinsdictionary.com/dictionary/english/cybercrime

Cybercrime. (2020). In Encyclopedia Britannica. https://www.britannica.com/topic/cybercrime

Cybercrime. (2020). In Merriam-Webster Dictionary. https://www.merriam-webster.com/dictionary/cybercrime

Cybercrime. (2020). In Oxford Advanced Learner's Dictionary. https://www.oxfordlearnersdictionaries.com/definition/english/cybercrime

Cybercrime. (2020). In The Chambers Dictionary. https://www.cybercrimechambers.com/blog-web-jacking-117.php

Geo News. (2017, December 4). Hundreds of Pakistanis lose millions in major ATM skimming fraud. Geo News. https://www.geo.tv/latest/170648-hundreds-of-karachiites-lose-millions-in-major-at-skimming-fraud

Government of Pakistan, Ministry of Information Technology and Telecommunication. (2018). Electronic Transactions Ordinance, 2002. http://www.pakistanlaw.com/eto.pdf

Government of Pakistan, Ministry of Information Technology and Telecommunication. (2018). Prevention of Electronic Crimes Act, 2016. http://www.na.gov.pk/uploads/documents/1470910659_707.pdf

Government of Pakistan, National Response Center for Cyber Crime. (2018). Cybercrime. http://www.nr3c.gov.pk/cybercrime.html

Johansen, G. (2020). Digital forensics and incident response: Incident response techniques and procedures to respond to modern cyber threats. Packt Publishing.

Lavorgna, A. (2020). Cybercrimes: Critical issues in a global context. Springer.

Littler, M., & Lee, B. (2020). Digital extremisms: Readings in violence, radicalization, and extremism in the online space. Springer Nature Switzerland AG.

Marion, N. E., & Twede, J. (2020). Cybercrime: An encyclopedia of digital crime. ABC-CLIO.

Pakwired. (2016, January 13). How secure are NADRA's critical information systems? Pakwired. https://pakwired.com/how-secure-are-nadras-critical-information-systems/

Tanveer, S., Manzar, U., & Jamal, S. (2016, June). The incidence of cybercrime in Pakistan. https://doi.org/10.13140/rg.2.1.1641.9448

Troia, V. (2020). Hunting cybercriminals: A hacker's guide to online intelligence gathering tools and techniques. Wiley.

Zaidi, M. (2015, February 14). FBI's most-wanted cybercriminal arrested in Karachi. Dawn. https://www.dawn.com/news/1163584