Analyzing the Cyberspace Laws to Protect Data Privacy in Pakistan

Submitted: 06.01.2021
Revised: 18.01.2021
Accepted: 28.01.2021

Article submitted to peer blind review

Naseem Razi*
ORCID: https://orcid.org/0000-0002-3466-0459
Rashida Zahoor**
ORCID: https://orcid.org/0000-0002-7991-6382
DOI: https://doi.org/10.26512/lstr.v13i2.35977

Abstract

[Purpose] Cyberspace technology has become an unavoidable forum for communications, connections, and transactions. This phenomenon, however, led to cybercrimes and hi-tech crimes such as data leaking, stealing, blackmailing, digital fraud, bullying and hacking, and all this has put the cyberspace technology at risk and a great threat to the security and privacy of the people. In Pakistan, cybercrimes are on the rise and despite several laws had been published on the topic, the rate of cybercrimes is increasing every passing year. In this context, this study examines the existing regulatory and legal framework for data protection in Pakistan and to find out the major challenges in the way of application and enforcement mechanism.
[Methodology] The conceptual framework of the research answers the question on to what extent the existing laws and enforcement mechanism of Pakistan is effective in protecting the data and information in the cyberspace? It highlights the importance of cyberspace technology nowadays and addresses the global agenda to combat cybercrimes, analyzes the Pakistani laws on the protection of data and privacy in cyberspace, and identifies major challenges in the way of the enforcement mechanism. The study focuses on the cyberspace laws of Pakistan with reference to the cybercrimes from a national perspective.
[Findings] This paper asserts that there is sufficient protection of cyberspace laws in Pakistan although they lack proper enforcement and are plagued with poor management.

Keywords: Cyberspace Technology. Cybercrimes. Pakistani Laws. Analysis. Recommendations.

INTRODUCTION

Cyberspace includes all the activities dependent upon technologies (PARKER, 1998). These technologies and network are running in a space known as cyberspace. In 1984, William Gibson used for the first time the term ‘Cyberspace’ in his Novel ‘Neuromancer’. At that time, this term was used to

*Associate Professor in Law, Department of Law, International Islamic University, Islamabad, Pakistan. E-mail: naseem.razi@iiu.edu.pk.
**Assistant Professor of Law, Department of Law, University of Sahiwal, Sahiwal, Pakistan. E-mail: rashidazahoor@uosahiwal.edu.pk.

elaborate the entire networks of digital technology and all the activities which take place or were performed with the help of the computer (STEVEN, 1990).

Currently, business, services, educational activities, entertainment, and communications are associated with the digital and information technology (DEMPSEY; GRABOSKY, PETER; and SMITH, 2001). Technologies are used to make business more effective and efficient and the services are being improved with the help of these technologies. For example, IT services are used in arranging online meetings, conferences and workshops and in transferring data from one computer to another (FED, 2000). These online services have not only limited the costs, but also saved the precious time of the individuals. Moreover, the physical exertion and energy is also hoarded with the use of such technology (KUNDI and NAWAZ, 2010).

Cyberspace in general and IT, in particular, are the weapons which empower the users worldwide to connect and to associate with each other (ALBERTS and PAPP, 1990).

This revolution, however, brought some perils and threats to the protection of data in cyberspace and thus, has opened a new path for serious crimes. The current digital revolution leads to invasion into privacy, hate speeches, data leaking, blackmailing, digital fraud, bullying, pornography, and hacking, etc (KUNDI, et al, 2010), which demands specific laws and an effective enforcement system to adopt preventive measures and to prevent crimes against cyberspace technology.

Taking this context into account, this article is divided into two parts. The first one explores cybercrime and the laws designed to protect the data in cyberspace from the global perspective. The second part goes further by way of discussing it in Pakistan. It also analyzes the existing legal framework to explore whether the existing legal structure is sufficient to cover each aspect of cybercrime. It also discusses some major challenges derived from proper implications and enforcement of the laws. In the end, some conclusions are drawn and some recommendations have been given to improve the system of security of data in cyberspace.

CYBERCRIMES: A THREAT TO THE PRIVACY OF DATA AND INFORMATION

The issue on how to protect data and information in cyberspace has become a key one to be solved as cyberspace has been more vulnerable to cyberattacks (HADNAGY, et al, 2014). Cybercrime is defined as a crime which is committed on the internet or some computer with the help of a software in order to destroy another computer or to gain information by way of stealing and hacking data (LEVI and HANDLEY, et al, 2002). Cybercrime is also termed as computer crime (HADNAGY, et al, 2014).

Cybercrime is categorized into three types. In the first type, computers are targeted as a prey to damage it or to destroy the information and data installed in a computer or other network system. In this category computers are bullied by forwarding infected software, malware, and viruses. In the second type, computers are utilized as a weapon. Online frauds, pornography, cyber stalking and cyber spoofing are the examples of this type. In the third type, computers are used as a repository to collect and to save the information and the data which are acquired by stealing and hacking (CLARKE and KNAKE, et al, 1962), (LEVI and HANDLEY, at al, 2002). For instance, withdrawal of the money from the 'Automated Teller Machine (ATM)' can put an individual in the danger of fraud and our bank account details and information on ATM cards can be copied by way of cybercrime. Similarly, online mode of filing taxes, refilling the prescriptions and internet-based financial services are also a source of electronic frauds of hacking and misusing of information (MARK, et al, 1996).

The extensive use of the internet and computers have increased the danger of privacy breach. Different forms of cyberattacks are being rapidly developed and people all around the globe have become victims of these crimes (PARKER, et al, 1998).

Public and government, both are at risk to become the target of the cyber criminals. Government critical infrastructure is a preferred targeted, but also the information of private actors and, specifically the banks is being stolen to gain financial advantages. In other cases, the corporations are attacked for some business gain (MARK, et al, 1996).

In order to control cybercrimes at domestic and global level, after the WWII, the US, the UK, Canada, Australia and New Zealand adopted a 'National Security Settlement' known as the 'Quadripartite', or 'United Kingdom - United States' (UKUSA) agreement (PARKER, et al, 1998).

The purpose of that agreement was to sign a bond in which a common 'National Security' may be attained. According to the understanding, the five countries divided the earth into five domains, and every nation was allocated specific targets. The UKUSA pact established phrasing, code words, care techniques, plans for collaboration, sharing of data, and access to services. One essential segment of the understanding was the trading of information and employees (see http://www.oispp.ca.gov/consumer_privacy/default.asp).

The idea to protect the data and information in cyberspace through legislation emerged in the 1970s (FLAHERTY, et al, 1998; PARKER, et al, 1998; BAMFORD, et al, 1981). Advanced technologies and devices expanded the need to draft legal framework for managing private information and data. Hence, many nations acknowledged the right to privacy in their legal structure (http://jya.com/stoa-atpc.htm). The United States of America enacted the 'Freedom of Information Act 1970' which allowed for the individuals to access their information at Federal Government Offices (PARKER, et al, 1998; LEVI and HANDLEY, et al, 2002).

In 1970, Germany adopted its first law regarding the protection of data and information in cyberspace. The right of data privacy was endorsed by Sweden in 1973. The US had also adopted this right in 1974 and France added it to the legal framework in 1978 (FLAHERTY, et al, 1989; PARKER, et al, 1998).

Developing countries may benefit from the ITU guidelines, which provide standards for the protection of online transactions and commerce. It helps the member states to draft such legislation which may be beneficial to control the cyber attacks, design the secured cyberspace and make cooperation with other states. It provides the security measures to protect the IT infrastructure (GERCKE, et al, 2012; PARKER, et al, 1998).

CYBERCRIMES AND CYBERSPACE LAWS IN PAKISTAN

Pakistan is ranked as the fifth most populated country in the world with more than twenty-two hundred million people (220,892,340). Around 62% of the inhabitants consist of youth between 18-24 years (see https://www.worldometers.info/population/countries). It is worth mentioning that Pakistan has an extended IT industry since the 1990s, which is considered a significant boost to the economic boom in the country in the coming years (KUNDI and NAWAZ, et al, 2010). Most of Pakistanis use digital technologies to interact with each other within and outside the country and Pakistan ranks in the list of top internet users (ZIBBER, et al, 2006).

The WORLD BANK REPORT (2013) showed that, in Pakistan, about 70% of the population use mobile phone to transfer and to receive the communication traffic while 11% population of them use the internet and its subscriptions. Internet reliance has made the communication information and data to be available in cyberspace (http://databank.worldbank.org). The World Bank Report (2014) estimated that Internet penetration in Pakistan reached 10.9 % in 2013. The Internet Service Providers Association of Pakistan (ISPAK) estimated 25 million Pakistani users in October 2014. Among them 11.6 million Pakistanis were on Facebook (http://content.bytesforall.pk).

In 2016, a survey carried out by GILANI RESEARCH FOUNDATION, (GALLUP PAKISTAN, 2016) pointed out that about 92% of the net users are regular consumers of social media (GILLANI, et al, 2016). The internet users are increasing rapidly, such as in June 2010, 99.19 million people were reported as internet subscribers while in May-June 2019 this number reached 161.18 million people (https://www.ncsc.gov.uk/events/cyberuk-2017).

SIMON KEMP REPORT (2020) revealed that about 76.38 million people are internet users, which is an increase of 17% since 2019. Meanwhile, the number of social media users was 34.6 million in 2019 which increased to 37 million people in 2020. Overall, in Pakistan, around 17% of the population use some form of social media and 164.9 million mobile connections were registered in 2020 which represents an increase of 6.2% since 2019 (SIMON KEMP REPORT, et al, 2020).

Social media websites like Facebook, Twitter, Blogs, MySpace, YouTube, Viber and WhatsApp are used for the purpose of communication, interaction and connectivity (http://www.pta.govpk/index.php). Another study conducted in 2019 pointed out that about 44.61 million people are internet users.

As far as the issue of cybercrimes is concerned, Pakistan is listed among those countries where the rate of cybercrime is increasing every year (https://www.ncsc.gov.uk/events/cyberuk-2017). The current situation is that in every 3 second, the identity of someone is stolen through cybercrime (http://www.nr3c.gov.pk/cybercrime.html).

The first ever cybercrime case was reported in 2003, which was relevant to the fake import, export business (ISLAM, KHAN, and ZUBAIR, et al, 2019). The Federal Investigation Agency has reported that 65% cybercrimes are committed on Facebook which includes blackmailing and harassment of women in which most of the cases are committed in Karachi (http://www.fia.gov.pk/en/index.php).

A study conducted by BYTES FOR ALL (2019) pointed out that, in 2018, about 90% of the cybercrimes were against women and girls, including minor girls while 70% of the cases involved pornographic content.

In 2002, only 10 to 15 cybercrimes cases were to be reported daily while, in 2020, more than 23 complaints were registered at the Cybercrime Wing on a daily basis (https://www.dawn.com/news/1475768).

To combat cybercrimes, Pakistan adopted its IT policy in 2000. The objective of this policy was to foster laws dealing with cybercrimes. For a comprehensive and best legislation, the "UNCITRAL Model Laws" and the legislations of various civil and common law countries were consulted and the "International Consensus Principals on Electronic Authentication" designed by the "Internet Law and Policy Forum" was considered a role model to be followed (KHAN, et al, 2014).

The "National IT policy and Action Plan (2000)" provides recommendations for making cyber laws to protect the privacy of individuals in the cyber domain (https://fdocuments.net/document/government-of-pakistan).

The "Electronic Transaction Ordinance 2002" was issued (http://www.pakistanlaw.com) to recognize and facilitate online business documentations, to keep records of communications and transactions in electronic forms, and to provide the accreditation of certification services. The Ordinance, however, could not cover all cybercrimes mentioned in various international cyber laws (www.home.kpmg).

For an efficient performance, Pakistan also signed a Mutual Legal Assistance (MLA) agreement with Kazakhstan in 2001, with Sri Lanka in 2006, with Uzbekistan in 2007, and with China in 2010 (http://www.na.gov.pk/uploads/documents).

In 2004, the 'Electronic Crimes Act 2004' was adopted in Pakistan to extend the scope of cybercrimes and to make some new cybercrimes punishable under the law (http://www.na.gov.pk/uploads/documents). The enacted law, however, could not cover the new cybercrimes in definite terms. The definitions of the cyber criminal acts were too vague (KHAN, et al, 2015). Moreover, it ignored the mechanism of implementation and could not establish any enforcement unit. Thus, the legislation proved useless (http://www.pakcon.org).

The 'Electronic Crimes Ordinance 2007' was another effort to bridge up the gap between the increasing cybercrime rate and the lack of proper legislation and enforcement mechanism. The scope of the Act extended to the whole of Pakistan and 17 types of cyber acts including cyber stalking and cyber spamming were declared cybercrimes and punishable by law (www.gov.pk/prevention-of-electronic-crimes-ordinance-2007).

The Ordinance was also criticized due to the vagueness of outlining the cybercrimes and due to severe sanctions against the mentioned crimes (https://propakistani.pk). The 'PILDAT Legislative Forum' also expressed its concerns by pointing out that "the offense of cyber-terrorism has been defined very broadly and that it carries a potential death sentence" (https://propakistani.pk/2009/10/27).

Until 2015, cyber space legislations could not be enforced effectively due to the aforementioned reasons.

On 16 December 2014, Pakistan faced its worst militant attack, and six terrorists attacked the Army Public School in the northwestern, city of Peshawar, killing more than 150 persons, out of them 132 were children (https://www.bbc.com/news/av/world-asia-35103616, 20-1-2021). That led to frame a 'National Action Plan 2015' to combat terrorist activities and cybercrimes (http://www.nagov.net, 20-1-2021).

Finally, 'The Prevention of Electronic Crimes Act 2016' was passed by the national assembly. The Act is applicable to the whole country and includes 7 chapters and 51 sections (http://www.na.gov.pk, 20-1-2021).

Chapter one of the Act 2016 is preliminary, contains 2 sections and describes jurisdiction and scope of the Act. It also presents definitions of different acts and authorities while chapter 2 deals with different types of the offence. It consists of 23 sections, among which sections 3-9 describe different forms of cybercrime like unauthorized access to information system or data (s.3); Unauthorized copying or transmission of data (s.4); Interference with information system or data (s.5); Unauthorized access to critical infrastructure information system or data(6); Unauthorized copying or transmission of critical infrastructure data (7); Interference with critical infrastructure information system or data (s.8); Glorification of an offense and hate speech(s.9), while section 10 declares these offences as cyber terrorism and subject to severe punishment which may extend to 14 years with or without fine (The Prevention of Electronic Crimes Act 2016).

Chapter 3 includes 12 sections and tackles the establishment of the investigation agency and powers of the investigation while chapter 4 includes only one section (s.39) and is about international cooperation. Chapter 5 consists of 5 sections. It is procedural in nature and is relevant to the prosecution and trial of offences. Chapter 6 is relevant to the preventive measures to avoid cybercrime and has 2 sections while chapter 7 deals with the miscellaneous matters and powers to make rules and consists of 4 sections (http://www.na.gov.pk, 20-1-2021).

To ensure cyber security and to protect data and right of the privacy, the Act 2016 has introduced some new cyber acts as crimes like illegal access of data by way of hacking, interference with data and information systems, electronic forgery and electronic fraud, cyber attack on the critical information infrastructure, unauthorized interception conducted by civilians, use of malicious code viruses, identity theft, etc.

Likewise, to curb cybercrimes extensively, the Act, authorized new investigative powers to the investigation agencies such as search and seizure of digital forensic evidence using technological means, production orders for an electronic evidence, electronic evidence preservation orders, partial disclosure of traffic data, real time collection of data under certain circumstances and other enabling powers which are necessary to effectively investigate cybercrime cases.

Like the prior legislations, the Act 2016 also got a lot of critique by the social and human rights activists who declared it a compromise of individual liberties and a restriction on the freedom of speech through surveillance, monitoring and censorship (QARAR, et al, 2018). Further, the powers vested in the investigation agency were also criticized by the stakeholders as it would lead to the misuse of the powers as witnessed in the earlier legislations. It is also important to note that under this Act, an agent of the investigation agency may arrest the offender without taking the warrant of arrest from the court.

It is, however, a matter of great concern that despite certain efforts and hard legislations, the issue of cybercrimes could not be reduced rather worsening every year. For instance, in 2014, the 'GLOBAL CYBER SECURITY INDEX' ranked Pakistan 23, which has been worsened alarmingly only within three years and in 2017, Pakistan ranked 67 which is an increase of about 150% (https://www.itu.int/en, 20-1-2021).

Looking into the hurdles and problems in the way of cyber security and data privacy, it is observed that inefficient and passive defense mechanism, the lack of e-forensic investigation, absence of professionals, incompatibility of the domestic laws, and incompetent enforcement mechanism are the big challenges in Pakistan (SALMAN, et al, 2018).

Another problem is that the system of spreading awareness and information is very weak rather ceased to exist. The education on cyber security is not efficiently provided in Pakistan. Only some institutions and universities are providing cybersecurity education. Moreover, the existing policy and scheme of studies in those institutions are not well designed to tackle the cyber security threats (HAQUE, et al, 2015).

The other challenge is the lack of proper training in cyberspace technology to protect data and privacy. Only few institutes provide trainings in the cyberspace technology, information security (AHSAN et al, 2014). For example, Pak-CERT is providing special training sessions to the corporate customers for security of digital information and preventing hacking. This team is also providing some professional education in the form of CISSP, network forensic, ethical hacking, penetration testing and computer security. It is also updating people to manage the security risks and to recover the damaged data and information (JUNIOR, 2018). Similarly, 'SKANS School of Accountancy' provides trainings and courses on information audit. It also awards certificates of 'Certified Information Systems Auditor (CISA)' to the trainees (ANDREJEVIC and GATES, et al, 2014).

The poor enforcement mechanism is also a great hurdle in the way of cyber security and data privacy. The cyber security system is very weak and based on poor management. Private and public data is at risk and is misused. For example, the 'Pakistan Internet Exchange' manages internet and communications on the internet within Pakistan. This system, however, was hacked by the 'British's intelligence agency GCHQ' in 2008 which gained access to Pakistan Internet Exchange and caused to threaten the right of privacy (https://digitalrightsfoundation.pk/press-release, 20-1-2021). Farooq Ahmed Khan Leghari (Late), the former president of Pakistan, claimed that the late Benazir Bhutto's second government was dismissed in the result of phone tapping (MCALONE, et al, 2016).

National Database and Registration Authority (NADRA) is the major biometric and centralized databases of the globe for the identity cards of the citizens of Pakistan (https://propakistani.pk/2015/11/26/nadra-has-issued, 19-1-2021). It has experienced much mismanagement along with data privacy breaches (http://profit.pakistantoday.com.pk/2017, 20-1-2021), fake registration of ID cards (https://www.dawn.com/news, 20-1-2021), and corruption by the officials of NADRA (https://pakwired.com/how-secure-are-nadras, 20-1-2021).

A report of the CITIZEN LAB (2014) revealed that various intrusion tools are used by different servers in Pakistan to collect the information from a remote computer system. The passwords are also cracked with the help of these tools. Sometimes the data is damaged by using malware. Moreover, a direct access is gained over others webcams and cell phones with the help of these dangerous intrusion trojans. These spywares include FinSpy, FinUSB and FinIntrusion Kit usually called FinFisher (https://www.dawn.com/news, 19-01-2021). In 2018, the data from Pakistani banks was hacked by cyber criminals (IQBAL, et al, 2018).

To improve the weak system of enforcement of laws, the 'National Response Centre for Cybercrime (NR3C)' has been established, the only unit under Federal Investigating Agency which deals with technology-based crimes. It not only directly receives complaints against cybercrime but also assists the other law enforcement agencies in their own cases (http://www.fia.gov.pk/en/NR3C.php, 19-01-2021). Likewise, the 'Virtual Private Networks (VPNs)' and encryption techniques were allowed to secure the data and the traffic information (bytesforall.pk › publication › Pakistan, 20-1-2021).

It is, however, encouraging news, that after the political change in Pakistan, the system of cyber security is getting better and a decline is observed in the cybercrime rate. For instance, in the financial cybercrime rate, a sharp decline has been witnessed in 2020, almost 50% despite the increase number of internet users during the year (http://www.technologyreview.pk, 20-1-2020).

The 'CYBERCRIME WING (Report 2020)', showed that in March 2020, almost 923 complaints were registered out of which 154 complaints were related to online banking frauds, 130 were against misuse of websites, 497 were about mobile banking, and 141 were linked to social media. While from March 23 to April 14, only 488 complaints were received against cybercrime. Among them, 89 were related to online banking frauds, 70 were linked to websites, 273 were to mobile banking, and only 50 were related to social media. During this two-month period (March-April 2020), the CCW also apprehended 45 accused cyber criminals and six infamous cybercrime gangs, while 39 formal cases were registered against them.

CONCLUSIONS

Cyberspace technology has become unavoidable as a means of development of the state. In this modern era, technological advancement has facilitated the emergence and advert of data privacy in cyberspace.

In Pakistan, the cyberspace is an emerging technology and has evolved in all the public and private institutions such as banks, educational departments, business sector and in the military sector.

Pakistan has overcome the issue of lack of proper legislation and has sufficient laws to protect data and privacy in cyberspace. Pakistan, however, is facing daunting challenges in the field of implementation of cyberspace laws for the purpose of cyber security and data privacy. The implementation mechanism is also weak.

Because of weak enforcement mechanism, the personal data of the state and the individuals, private and public is not secured.

RECOMMENDATIONS

This paper recommends improving the implementation mechanism in cyberspace and to enforce cyberspace laws in Pakistan. The 'National Response Centre for Cybercrime (NR3C)' should adopt an effective cyber security policy to protect the privacy of data on the one hand and to protect Pakistan from the evils of cyber warfare.

This study also recommends proper training to the 'Computer Emergency Response Team (CERT)' by highly skilled professionals to combat the present challenges of cyberspace and threats to informational privacy.

The educational institutions should also be bound to disseminate awareness regarding cybercrimes and cyber security and to educate them to protect their personal information in cyberspace. Specially, the teenager girls, children, young boys and working women should be made aware of data protection to protect their personal data on digital devices.

The business communications and banking transactions may be protected by an effective enforcing system. Similarly, institutions should have their own cyber laws to conduct their communications in safe hands.

REFERENCES

Alberts, D. S.; Papp, D. S. (1997). *The information age: An anthology on its impact and consequences.* Office of the Assistant Secretary of Defense Washington DC Command and Control Research Program (CCRP).

Amoore, L. (2014). Security and the claim to privacy. *International Political Sociology,* 8(1), p. 108-112.

Andrejevic and K. Gates. (2014). Big Data surveillance: *Introduction. Surveillance & Society,* 12(2), p. 185-196.

Bamford, James. (1981). *The Puzzle Palace*. Penguin Books.

Bell, R. E. (2002). The prosecution of computer crime. *Journal of Financial Crime,* 9(4), p. 308-325.

Britz, M. T. (2008). A New Paradigm of Organized Crime in the United States: Criminal Syndicates, Cyber-gangs, and the Worldwide Web. *Sociology compass,* 2(6), 1750-1765.

Bytes for All Pakistan. (2013). Report 2013. *Pakistan's Internet Landscape.* Available at: http://content.bytesforall.pk.

Clarke, R. A.; Knake, R. K. (2010) *The Next Threat to National Security and What to Do About It.* New York: Ecco.

Cyber Crime Wing (CCW). (2020). Report 2020. Available at: http://www.technologyreview.pk.

Dombrowski, S. C.; Gischlar, K. L.; Durst, T. (2007). Safeguarding young people from cyber pornography and cyber sexual predation: A major dilemma of the Internet. *Child Abuse Review: Journal of the British Association for the Study and Prevention of Child Abuse and Neglect*, 16(3), p. 153-170.

European Parliament. *Scientific and Technological Options Assessment (STOA).* An Appraisal of Technologies of Political Control. 6 January 1998. Available at: http://jya.com/stoa-atpc.htm.

Fidelie, L. W. (2009). Internet gambling: Innocent activity or cybercrime? *International Journal of Cyber Criminology,* 3(1).

Flaherty, David. (1989). *Protecting privacy in surveillance societies:* The Federal Republic of Germany, Sweden, France, Canada, and the United States. Chapel Hill, The University of North Carolina Press.

Frieden, J. D.; Murray, L. M. (2011). The admissibility of electronic evidence under the federal rules of evidence. *Richmond Journal of Law & Technology,* 17(2).

Gercke, M. (2012). *Understanding Cybercrimes*: Phenomena, Challenges and Legal Response. International Telecommunication Union.

Gillani Research Foundation. (2016). Gallup. *Opinion Poll Information Technology Computer/Internet*. Available at: http://gallup.com.pk/.

Grabosky, P.; Smith, R. G.; Smith, R. G.; Dempsey, G. (2001). *Electronic theft: Unlawful acquisition in cyberspace.* Cambridge: Cambridge University Press.

Hadnagy, C. (2014). *Unmasking the social engineer*: The human element of security. John Wiley & Sons.

Haque, Jahanzaib. (2015). *Developing a Progressive Internet Policy for Pakistan*. Policy Brief, Jinnah Institute.

Iqbal, Shahid. (2018). *Around 10 banks block international payments on debit and credit cards*.

Islam, Z. U.; Khan, M. A.; Zubair, M. (2019). *Cybercrime and Pakistan. Global Political Review*, 4(2): 12-19.

Jamil, Zahid. (2006). Cyber Law. Presented at the *50th anniversary celebrations of the Supreme Court of Pakistan International Judicial Conference*,11-14 August, 2006.

Junior, Moneeb. (2018). Cyber Secure Pakistan 2018, presented at the *International Cyber Security Conference held in Islamabad*, 29 March 2018.

Khan, Khalil-ur-Rehman, Cyber Laws in Pakistan. Available at: https://www.scribd.com/document/203767010/Cyber-Laws-Pakistan.

Khan, Talha. (2015). Cybercrimes: Pakistan lacks facilities to trace hackers. *The Express Tribune*.

KPMG Forensic and Litigation Services. (2013). *Report 2013. Global eFraud Survey*.

Kundi, G. M.; Shah, B.; Nawaz, A. (2008). Digital Pakistan: opportunities & challenges. *JISTEM-Journal of Information Systems and Technology Management*, 5(2): 365-390.

Kundi, G. M. (2010). *E-Business in Pakistan:* Opportunities and Threats. Lap-Lambert.

Levi, M.; Handley, J. (1998). *The prevention of plastic and cheque fraud revisited*. London: Home Office.

Luiijf, H. A. M.; Besseling, K.; Spoelstra, M.; De Graaf, P. (2011). *Ten national cyber security strategies:* A comparison. International Workshop on Critical Information Infrastructures Security. Springer, Berlin, Heidelberg.

Mohiuddin, Zibber. (2006). Cyber Laws in Pakistan: A Situational analysis and Way Forward. *Ceericsson Pakistan*.

Nathan, McAlone. (2016). *The 15 Companies that Flooded your Inbox with the Most Email Spam in 2015*. Business Insider.

National Research Council. (2010). *Deterring Cyberattacks:* Informing Strategies and Developing Options. Proceedings of a "Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Committee.

Nureni Ayofe, A.; Oluwaseyifunmitan, O. (2009). *Approach to Solving Cybercrime and Cybersecurity.*

PakWired. (2016). *How Secure Are NADRA's Critical Information Systems?*

Pakistan Advertisers Society. (2014). *Annual Social Media Marketing Infographics 2014*.

Pakistan Telecommunications Authority (PTA). (2014). *Report 2014. Cellular Mobile.* Available at: http://www.pta.gov.pk/index.php?Itemid=135.

Pakistan Today. (2017). *SBP looking into NADRA-MasterCard agreement over concerns of possible breach of security of national database*. Available at: http:// profit.pakistantoday.com.pk/2017/01/26/sbp-looking-into-nadra.

Parker, D. B. (1983). *Fighting computer crime.* New York, NY: Scribner.

ProPakistani. Report 2015-16. *NADRA Has Issued 101 Million ID Cards, Blocked 125K Fake Cards.* Available at: https://propakistani.pk/2015/11/26/nadra-has-issued-101-million-id-cards-blocked-125k-fake-cards.

Qarar, Shakeel. (2018). Around 10 banks block international payments on debit and credit cards. The Express Tribune.

Rahman, T. (2014). *The internet, youth and education in Pakistan.* UNDP Pakistan.

Rasch, M. (1996). Criminal law and the internet. The Internet and Business: A Lawyer's Guide to the Emerging Legal issues. *Computer Law Ass*, 1996.

Rengert, G. F. (2004). The journey to crime. Bruinsma, G., Elffers, H., Willem, J., de Keijser (Eds.) *Punishment, Places, and Perpetrators: Developments in Criminology and Criminal Justice Research*, p. 169-181.

Shah, Aaushi and Srinidhi. (2012). A to Z of Cyber Crime. *Pune: Asian School of Cyber Laws*.

Siddiqui, Salman. (2018) Banks being hit by cyber attacks FIA. *The Express Tribune*.

Simon Kemp. (2020) *Digital 2020: Pakistan.* Available at: https://datareportal.com/reports/digital-2020-pakistan.

The Dawn (2014). *Customer 32 - who used FinFisher to spy in Pakistan?* Available at: https://www.dawn.com/news/1127405.

World Bank Report (2013). *Pakistan: Internet users per 100 people.* Available at: http://databank.worldbank.org/data//reports.

The Law, State and Telecommunications Review / Revista de Direito, Estado e Telecomunicações

Contact:
Universidade de Brasília - Faculdade de Direito - Núcleo de Direito Setorial e Regulatório
Campus Universitário de Brasília
Brasília, DF, CEP 70919-970
Caixa Postal 04413

Phone: +55(61)3107-2683/2688

E-mail: getel@unb.br

Submissions are welcome at: https://periodicos.unb.br/index.php/RDET