



The Contested Nature of Cyber Crimes and Identity Theft: A Case of Balancing Security and Privacy in Pakistan's Cyber Laws

Syed Raza Shah Gilani

Assistant Professor of Law at Abdul Wali Khan University Mardan, Pakistan. Journal of Islamic State Practices in International Law

Zahid Ullah

Lecturer in Political Science at Abdul Wali Khan University Mardan, Khyber-Pakhtunkhwa, Pakistan.

Abdus Samad Khan Marwat

Assistant Professor of Law Abdul Wali Khan University Mardan, Pakistan.

Vol. 4. No. 1/2022

The IJKS

provides a forum for scientific exchange and public dissemination of up-to-date scientific knowledge on the Kashmir conflict, The IJKS is an independent, peer-reviewed, open-access journal.

The topics on which we concentrate—Kashmir conflict and violence—have always been central to various disciplines. Consequently, the journal encompasses contributions from a wide range of disciplines, including international affairs, political studies (geopolitics, political economy and other dynamics, diplomacy and public advocacy, law-based approaches, governance and economy (including micro and macroeconomics), self-determination, and other solidarity rights public international law (including human rights and humanitarian laws and intergovernmental organizations), criminology, economics, education, ethnology, history, political science, psychology, social anthropology, sociology.

All articles are gathered in yearly volumes, identified by a QR Code in print volume with article-wise pagination. For more information, please visit www.kprijk.org

Suggested

APA: Ahmad, I., Ali, Marriam. (2021). Pro-Environment Workforce: Studying Employee Behavior in the Pharmaceutical Companies of at the Sundar Industrial Estate. International Journal of Kashmir Studies, 6.

Citation:

Harvard: Ishtiaq, Ahmad. Marriam Ali. (2021). Pro-Environment Workforce: Studying Employee Behavior in the Pharmaceutical Companies of at the Sundar Industrial Estate International Journal of Kashmir Studies, 6.



The Contested Nature of Cyber Crimes and Identity Theft: A Case of Balancing Security and Privacy in Pakistan's Cyber Laws

Syed Raza Shah Gilani

Assistant Professor of Law at Abdul Wali Khan University Mardan, Pakistan. Journal of Islamic State Practices in International Law

Zahid Ullah

Lecturer in Political Science at Abdul Wali Khan University Mardan, Khyber-Pakhtunkhwa, Pakistan.

Abdus Samad Khan Marwat

Assistant Professor of Law Abdul Wali Khan University Mardan, Pakistan.

Abstract

There is no denying the fact that human beings have become too dependent on technology. Based on a study conducted by the United Nations Office on Drugs and Crime, around 30 percent of the world's population has access to the internet and currently 70% of the world population has mobile and broadband subscriptions. The downside of the increase in the number of connecting devices and sophistication in information technology is an increase in the number of computer-mediated problems. Cyberspace is a term used to describe the virtual 'geography' of the internet. Computer technology and networking innovations have undoubtedly given rise to what some have described as a 'borderless' and network society which enables instantaneous communication between private individuals, governmental authorities and businesses. That is to say, the usual boundaries of communication do not apply to the "cyberspace," as the internet does not occupy any physical space. Transactions can be initiated in one country, processed in another, and concluded in yet another.

Consequently, actions and processes that are conducted in the cyberspace will often not fall under the legal control and jurisdiction of a single state. This article examines these computer-related challenges.

Key Words: Cyber Space, Network Society, Cybercrimes, Computer Technology, Cyber Laws

Introduction

Innovations in information and communication technologies have not only brought facilities for human life but also opened new channels for “identity theft” and fraud. Identity thieves can impersonate the dead as well as the living. In other words, identity theft happens “when someone uses your personal identifying information and pretends to be you in order to commit fraud or to gain other financial benefits.”¹ Identity theft and fraud include: “false applications for loans and credit cards, fraudulent withdrawals from bank accounts, fraudulent use of telephone calling cards or online accounts, or obtaining other goods or privileges which the criminal might be denied if he were to use his real name.”² Additionally, offenders can steal credit card details, withdraw savings from personal accounts, or take out loan applications and mobile phone accounts in another person’s name. These acts involve some form of identity impersonation. But in many cases, they also involve some prior data breach (e.g., some form of intrusion on computer networks) that facilitates the misuse or unauthorized access to personal information.³

¹ J.V. Kleut, “Norton Life Lock.” n.d. <https://us.norton.com/internetsecurity-id-theft-what-is-identity-theft.html>

² The United States Department of Justice. “What are Identity Theft and Identity Fraud.” November 16, 2020. <https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud>

³ Mike McGuire & S.Samantha Dowling, “Cyber Crime: A Review of the Evidence: Summary of Key Findings and Implications,” *Home Office Research Report*” Report no. 75, (2013): 5-7.

The concept of “identity theft” is still contested. The upsurge in identity related incidents have generated a legal debate about what precisely constitutes an act of identity theft. There is also some confusion over the ‘true’ ‘victim’ of such crimes. For example, scholars disagree over whether a legal distinction can be made between account takeovers and “true name fraud.” Account takeover or ‘hijacking’ refers to a type of identity theft where a fraudster obtains unauthorized access to multiple online e-commerce account using bots or means of hacking and system interference.⁴ Bots in particular extract information on a random basis.⁵ In such cases, the bank account takeover attacks are, in the first sense, an attack on the critical infrastructure of a banking institution. While the bank bears the primary costs of online bank takeovers, the account holder suffers consequential losses from the original system interference offence. A successful account takeover occurs when an offender obtains enough information to carry out unauthorized transactions in the victim’s name or transfer funds to third-party accounts using the compromised account,⁶ and banks are usually liable for losses that directly result from ‘hijacked’ bank servers and payment systems.⁷

A real fraud is said to have occurred when some form of impersonation-related deception is involved. This typically occurs when credit card information is stolen from a victim directly and used to make purchases in the cardholder’s name. In such cases, the only

⁴ Aliza Vigderman, “Account Takeover Fraud: A Consumer’s Guide to Protecting Yourself,” *Security.org*, <https://www.security.org/digital-safety/account-takeover-prevention/>

⁵ Pooja Aggarwal, et.al, “Review on Cyber Crime and Security,” *International Journal of Research in Engineering and Applied Sciences*, 2(1), (2014): 48-51.

⁶ Graeme R. Newman, & Megan M. McNally “Identity Theft Literature Review,” U.S. Department of Justice, (2005), <https://www.ojp.gov/pdffiles1/nij/grants/210459.pdf>

⁷ Hemraj Saini, Year Shankar Rao, & T.C. Panda, “Cyber-Crimes and their Impacts: A Review,” *International Journal of Engineering Research and Applications*, 2(2) (2012): 202-209.

recourse available to the credit card holder is to contact the issuing bank which then initiates a chargeback dispute with the aim of recovering the fraudulent charges on their card. It is apt to note that their losses in terms of money are not only far bigger in proportion, but are also harder to uncover, and take significantly longer time to resolve.⁸ Account and/or card theft therefore exposes the account holder to a psychological trauma that is much more harmful than the theft itself.

While existing data demonstrates that financial identity theft and fraud are a significant problem, it is also possible to suggest that statistics on cybercrime are skewed towards a particular sub-set of financial crimes, such as credit card theft. The preoccupation with a credit card and financial fraud tends to overshadow the legal issues in dispute. The next section sheds some light on the key points of distinction and disagreement over the impact of online fraud targeted at companies versus individuals; the theft of identity ownership versus theft of property, or the legal boundaries between “identity theft” versus “identity fraud.” It will consider these issues in the context of existing literature, legislation, and relevant policy debates.

The Concept of Identity in Identity Theft

Scholars such as Robinsons and others argue that a person’s identity is universally recognizable as a category of personal property or as an intangible quality. Identity ownership is a key element of personhood and citizenship in areas such as taxation, national security, immigration, and crime, among others. Identity can take numerous forms, such as documents or a set of data, whose primary purpose is

⁸ Office for Victims of Crimes, “Expanding Services to Reach Victims of Identity Theft and Financial Fraud,” October 2010, https://ovc.ojp.gov/sites/g/files/xyckuh226/files/pubs/ID_theft/pfv.html

to establish a person's unique characteristics.⁹ Scholars differ on how to differentiate between "identity" and the more distinct concept of "identification," (e.g., generic information that can be utilized to recognize individuals). These issues will be discussed in a later section on the use of big data and its impact on individual privacy, etc. For the moment, it is important to note that there is also a debate on how "identity" is being used in relation to terms of traditional definitions of crime, theft, and fraud.¹⁰

As noted, it has been previously assumed that theft cannot occur unless an "actual thing" is stolen, thereby resulting in "a deprivation to the owner."¹¹ In the age of information-centric crime, most legal systems have taken steps to outlaw data theft used for the purposes of carrying out fraud using another person's identity. However, the criminalization of identity theft and fraud offences are often conflated with the cost of legal clarity on the interests protected by each of these offences. The tendency to elide the distinction between identity related offences with traditional financial crimes also overlooks the idea that the loss or deprivation of identity and identity ownership implies something more than just the loss of a digital asset.¹² Given its critical role in daily aspects of life and its universal nature, the illegal or unauthorized use of a person's identity represents a very serious threat to an individual's privacy, security and autonomy.

Computer-generated attacks on the integrity and confidentiality of online information may also be carried out for non-economic reasons,

⁹ Peter J. Spiro, "A New International Law of Citizenship," *The American Journal of International Law*, 105(4) (2011): 700–705. doi: <https://doi.org/10.5305/amerjintlaw.105.4.0694>

¹⁰ McGuire & Dowling, "Cyber Crime: A Review of the Evidence," 4-5.

¹¹ Ishita Khurana, "Does Copyright Infringement Fall within the Traditional Definition of Theft?: An Indian and International Analysis," June 5, 2020, *Center For Criminal Law, NUSRL, Ranchi*.

¹² McGuire & Dowling, "Cyber Crime: A Review of the Evidence," 16-17.

particularly in the sphere of identity-related larcenies.¹³ Offenders may seek to intercept private communications or create imposter social media accounts using the identity of another with the specific aim of damaging their reputation or manipulating identification documents such as criminal or credit records. These forms of or data interception and impersonation fraud may have lasting effects on the victim's future employability and financial prospects.¹⁴ These and other factors complicate our understanding of identity theft as some individual and identity-centered phenomena while differentiating it from existing definitions of online credit card and account fraud.

Existing Definitions of Online Identity Theft

One of the main reasons why scholars, and law-makers, have not been able to reach consensus around a definition of identity theft is because it rarely manifests as a stand-alone crime, but is often committed as part of a larger criminal enterprise.¹⁵ Thus, the question for lawyers is: at what point in a series of computer-mediated offences does an individual or group actually commit identity theft? Identity-related larceny occurs, according to the Organization for Economic Co-operation and Development (OECD), when an individual and/or a group illicitly collects and uses the information of an existing individual (whether legal or natural) with the intention of committing fraud or other criminal activities.¹⁶ This legal test would seem to establish a link between some initial act of illegal access and data acquisition, with the "financial gain" element of traditional

¹³ United Nations Office on Drugs and Crime, "Computer-Related Offences, *n.d.* <https://www.unodc.org/e4j/zh/cybercrime/module-2/key-issues/computer-related-offences.html>

¹⁴ Judge Mohamad Chawki & Abdel Wahab, "Identity Theft in Cyberspace: Issues and Solutions," *Lex Electronica*, 11(1) (2006): 2-3.

¹⁵ Newman & McNally, "Identity Theft Literature Review," 5.

¹⁶ Organisation for Economic Cooperation and Development, "OECD Policy Guidance on Online Identity Theft," Seoul: OECD Ministerial Meeting on the Future of the Internet Economy, (2008).

definitions of theft and fraud.¹⁷ Some scholars provide a narrower definition of theft related to identity by focusing on the element of impersonation as a key element of this offence, thereby distinguishing it from other forms of traditional conceptions of economically motivated and property-based crimes.¹⁸ What is important to note in the occurrence of identity-related theft, according to Jan Grijpink, is that the perpetrator must, for malicious or criminal purposes, assume an identity that is not his or hers.¹⁹ What could be inferred from this discussion is that an individual or group accused of identity theft can only be successfully prosecuted if the following criteria are met: 1) the act of obtaining private information must have been acquired through illegal means, 2) for the accused's (financial) gain and c) by means of impersonating as someone else.

Experts in the field such as Newman and McNally have expanded on the above criteria to identify three components of identity theft that should be analyzed from a law enforcement perspective. The first refers to the commonality of criminal intent between an initial act of obtaining personal information and some future intention to commit identity theft. A second dimension relates to the degree of criminal liability— that is, to apportion blame to persons who aid and abet fraud offence. For example, how liable is the person involved in a system interference attack but who plays no further part in a later financial fraud i.e., the hacker who hijacks an online account and then sells these details on to third parties? The third factor concerns the variability of outcome and its relation to the discovery of the crime.²⁰ This refers to the fact that personal identification data may be unlawfully accessed and obtained some time before a financial loss is

¹⁷ United Nations Office on Drugs and Crime,

¹⁸ Thomas King, et.al., "Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions," *Science and Engineering Ethics*, 26, (2020): 98-99

¹⁹ Jan Grijpink, "Privacy Law: Biometrics and Privacy," *Computer Law & Security Review*, 17(3) (2001): 154-160.

²⁰ Newman & McNally, "Identity Theft Literature Review," v.

discovered by the victim and subsequently reported to the relevant authority.²¹

As noted above, one of the most significant obstacles to the formulation of a workable definition of identity related offences is that these are often inseparable from some original preparatory act of unlawful data gathering, acquisition or system interference. However, the methods used, and motivation behind these acts, vary greatly. In the case of “account takeover” for instance, the act of unlawfully acquiring personal details relating to a specific account holder is an end of itself. In so-called ‘synthetic’ identity theft, offenders blend information relating to any individual with ‘fabricated’ data for the purpose of setting up fake accounts. In other cases, offenders use automated techniques to ‘hack’ data relating to thousands of anonymized accounts is hacked and extracted through malicious software, a technique known as spear phishing.²² In these cases, the offender may have no further involvement than to extract information which is then sold to gangs on the black market. Under current definitions, this would not be a direct case of identity theft since the offender does not “impersonate” another person, nor would he necessarily benefit from the act of stealing information.²³ These types of crimes are also harder to discover since a true name fraud may not occur till sometime after the information was unlawfully accessed. The anonymity of offenders, combined with the difficulty of proving a causal link between account theft and some subsequent fraud against an individual, are significant factors in the low-rate of identity theft related convictions.

²¹ United Nations Office on Drugs and Crime.

²² Todd Jones, “Synthetic Identity Theft: The New Way Your ID Gets Stolen,” Aura, <https://www.aura.com/learn/synthetic-identity-theft-fraud>

²³ Syed Raza Shah Gilani & Hidayat Ur Rehman, “The Principles of “Necessity” and “Balance”: the Most Important Elements of the Doctrine of Proportionality in the” Judicial Review Process,” *Dialogue (Pakistan)*, vol.15, Issue 3 (2020): 112-35.

Distinguishing Identity Theft and Identity Fraud

As discussed earlier, there is no clearcut line that differentiates technological offences from traditional crimes, other than the means through which digital offences are committed. Not only does identity theft related jurisdictions vary, but so too does the terminologies in use, i.e., identity fraud, identity theft, for such crimes. Identity theft is a criminal offence in most jurisdictions, though there is significant variation in the relevant legal and definitional criteria used to indict such offences.²⁴ For example, in the United States, identity theft is criminalized under the 1998 Federal Identity Theft and Assumption Deterrence Act of 1998, 18 USC. The crime is defined by the provisions of this Act as any activity whereby an individual or group:

knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable state or local law.²⁵

This definition of identity theft has been criticized as being too expansive, since it offers no way of distinguishing online fraud, primarily credit card fraud, from identity theft involving some additional element of impersonation. This does not resolve the question of whether non-economically motivated impersonation of an individual's identity is sufficient to meet the criteria of criminal identity theft. Take the case of a deceptive profile on a dating website or the unlawful access to private information or highly sensitive images stored on cloud networks which are then posted onto a public domain website for 'revenge' purposes. These activities do not necessarily result in some direct economic loss for the victim though they have been motivated by the offender's intention to inflict

²⁴ Megan Wyre, David Lacey, & Kathy Allan, K. "The Identity Theft Response System," *Trends & Issues in Crime and Criminal Justice*, Australia, No. 592 (2020): 15-16.

²⁵ Newman & McNally, "Identity Theft Literature Review," 1.

emotional ‘harm’ on a victim or otherwise defame their character. It is not obvious that such acts would be covered by the relevant US criminal statutes and restitution laws.²⁶ In any case, aggravated penalties for virtual crimes tend to be reserved for financial crimes, especially those involve large scale credit card and banking fraud.

The UK Home Office has defined identity related offences in more information-centric terms as an offence that is committed when somebody gets a substantial amount of information about a person’s identity that assists identity-related theft. Notably, the UK government has emphasized “fraud” as a constitutive element of identity related offences as opposed to the word “theft”. It is arguable that the reference to “fraud” under the current provisions of UK law bypasses longstanding debates on how criminal law should regulate the boundaries between theft and misuse of information properly.²⁷ By avoiding the question of the conditions under which illegal access to personal information qualifies as an act of “theft”, the terminology of “identity fraud” has the advantage of dealing with a wide range of data privacy violations.²⁸ This concept of identity fraud would, for example, cover the deliberate act of obtaining goods and services under a false name (a non-existing person). What is less clear is whether identity fraud offences can be established by the simple act of extracting identifying information about a person without their consent? Or would this constitute an overly broad definition that that would bring relatively ‘harmless’ acts, such as commercial use and transfer of data, within the scope of criminal law?

Some scholars have remarked on the differences between the US and the UK in this regard. The US, it is argued, treats identity theft as a

²⁶ Harjinder Singh Lallie, et.al., “Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic,” *Computers & Security*, 105 (2021): 2-9.

²⁷ Arjan Reurink, “Financial Fraud: A Literature Teview,” MPIfG *Discussion Paper no. 16/5*, Cologne: Max Planck Institute for the Study of Societies, (2016): 64-69.

²⁸ Lallie, et.al., “Cyber Security in the Age of COVID-19,” 13.

distinct offence while the UK tends to conceptualize these offences as a technological variant of general fraud offences. The US definition of identity would exclude, by implication, the simple act of acquiring, through unlawful means, personal information relating to personal identity. Some further act of impersonating a specific person using 'stolen' information would need to have occurred beforehand. However, this narrow formulation of criminal identity theft would also preclude, for instance, the use of anonymized 'bots' that may be used to generate a profile of individual users. Once data profiles have been created, a person's anonymity is compromised. In addition to violating individual privacy, identity and data ownership, this information can also be accessed and exploited for fraud purposes. On the other hand, it should be emphasized that while the UK formulation of identity fraud covers a broader range of data violations it also denotes a certain type of economically motivated crime.²⁹ The difficulty with this definition is that it would seem to place non-financially motivated identity theft offences outside the legitimate sphere of criminal law and penal philosophy.

Data Privacy Protection

While identity theft is ultimately an offence against the individual and individual privacy, it is most likely to thrive on an integrated information economy. In an integrated global economy, more people are willing to enter into contracts to sell goods and services to anonymous buyers. This, in turn, has accelerated retailer's dependency on consumer data for credit verification purposes. The ease with which data is shared also makes it easier for criminals to use the information for theft and fraud purposes. The use of online shopping websites has made it easier to collect and analyse consumer data. Most legitimate sites do not solicit consumers to input confidential financial and will install two-step authentication systems, however, identity thieves can use other methods of social deception

²⁹ Chawki & Wahab, "Identity Theft in Cyberspace," 6.

including pharming and phishing to fill in the blanks.³⁰ In this regard, identity theft flourishes when a person or group with criminal intent obtain enough information about a chosen victim to “counterfeit this link, enabling the thief to acquire goods while attributing the charge to another person's account,” which expose the personal information of the customers.³¹

As alluded to above, the sharp rise in credit card theft is, however, only the tip of the iceberg. Data is and will continue, to be a valuable currency in the decades to come, while also fundamentally transforming the relationship between individuals, governments, and the private sector. Many ‘big data’ companies collect large amounts of data for marketing purposes.³² John Marshey is considered to be the first person who used the term “big data”—that is, an enormous set of data. The market in data collection was estimated to be worth around 203 trillion dollars as of 2017.³³ This shows how valuable this industry has become—big data now outpace oil commodities in value. At the same time, the rise of cloud computing has transformed the way companies transfer and store personal data. A vast amount of personal data is being collated, processed, transferred, and stored, for instance, in offshore databases via virtual cloud-computing networks. The popularity of cloud computing services generates obvious privacy related concerns around a company’s ability to sell, collect or transfer private data without the subject’s consent.³⁴

³⁰ Zainab Alkhalil, Hewage Chaminda, H., Liqaa, Nawaf & Imtiaz Khan “Phishing Attacks: A Recent Comprehensive Study and a New Anatomy,” *Frontier in Computer Science*, 3 (2021): 15-17. doi:10.3389/fcomp.2021.563060

³¹ Keith B Anderson, Erik Durbin, and Michael A Selinger, “Identity Theft,” *Journal of Economic Perspective*, Vol.22, Issue. No.2, (2008): 171-72.

³² Alla Morrison, “Attention Governments: Big Data is a Game Changer for Businesses,” *World Bank Blog*, <https://blogs.worldbank.org/opendata/attention-governments-big-data-game-changer-businesses>

³³ Gil Press, “6 Predictions for the \$203 Billion Big Data Analytics Market,” *Forbes*, January20, 2017, <https://www.forbes.com/sites/gilpress/2017/01/20/6-predictions-for-the-203-billion-big-data-analytics-market/?sh=12114a9e2083>

³⁴ Sompurna Bhadra, “Cloud Computing and Privacy Risks in the Information/Knowledge/Digital Risk Society and Economy: An Overview,”

Many companies claim that they safeguard the identity of the individual by collecting data that is ‘anonymized.’³⁵ That is to say, without associating that data sets to specific individuals. There is nothing inherently new about the use of ‘anonymous data-based transactions’ since credit card payment verification systems have long relied on these methods.³⁶ However, in the current age of cloud computing and data profiling, anonymization is near impossible to achieve, and is, moreover, increasingly susceptible to reverse engineering methods. Big data analysis can be traced back to individual users through re-identification methods (since digital information carries its own signature). To take one example, the internet provider AOL disclosed data relating to 20 million Internet search results for research purposes. To protect the personal identities of its customers, AOL replaced usernames with a random number.³⁷ But internet cryptographers were able to use reverse engineering techniques to determine the identity of anonymized AOL customers.³⁸

Big data analysis and data mining techniques, combined with the vast amounts of personal data made available on the internet, creates the very conditions under which identity theft can thrive. It has also been established that new payment systems and flows of data have undermined individual privacy. However, data flows can also provide solutions to threats, as well as being the source of these threats. Cybersecurity companies rely on large sets of impersonalized data to

International Journal for Research in Applied Science & Engineering Technology (IJRASET), 8(VI), (2020): 2244-45.

³⁵ Alex Hern, “Anonymised Data can never be Totally Anonymous” *The Guardian*, July 23, 2019,

<https://www.theguardian.com/technology/2019/jul/23/anonymised-data-never-be-anonymous-enough-study-finds>

³⁶ Bhadra, “Cloud Computing and Privacy Risks in the Information/Knowledge/Digital Risk Society and Economy,” 2225 & 2244.

³⁷ Michael Arrington, “AOL Proudly Releases Massive Amounts of Private Data,” *TechCrunch*, August 7, 2006, <https://techcrunch.com/2006/08/06/aol-proudly-releases-massive-amounts-of-user-search-data/>

³⁸ Bruce Schneier, “Why ‘Anonymous’ Data Sometimes Isn’t,” *Wired*, December 12, 2007, <https://www.wired.com/2007/12/why-anonymous-data-sometimes-isnt/>

analyze threats based on the information gathered. How then can data privacy and protection be achieved while sacrificing flexibility, accessibility, and innovation in ICT sectors? This trade-off will be briefly discussed in the next section regarding the extremes of broad and narrow legislative approaches to data protection within the broader cybersecurity debate.

Blurred Boundary between Data Protection and Criminalization

The above-mentioned regimes, however, have historically been conceived as separate and segmented from broader approaches to criminal law. The arena of internet governance breaks down the usual boundaries set up between international and domestic norms and public and private legal spheres. It also collapses the distinction between civil law-governed data breaches and criminal law definitions of theft and fraud. In most legal systems, an act of transferring or using personal data would not amount to a crime, without some additional evidence of criminal purpose and intent. Nonetheless, it is also clear that no sharp line separates an original act of unauthorized access and misuse of data and a subsequent “crime” of theft or fraud. From this vantage point, the information era raises difficult questions about the role of user consent in data use or transfer (can a person “steal” private data if the user has posted information on any social media platform.³⁹ Similarly, debates on data misuse reopen longstanding debates about the scope of the law in criminalizing data breaches, or how companies should handle and process personal data.

Responding to the increasing identity-related offences, some scholars advocate for a legal definition of cybercrime that does not hinge upon physical means through which crime is committed i.e., computer hardware or networks, but on the value and utility of the personal

³⁹ Mathew B. Prince, et.al., “Understanding How Spammers Steal Your E-Mail Address: An Analysis of the First Six Months of Data from Project Honey Pot,” *Proceedings of the Second Conference on Email and Anti-Spam (CEAS)*, (2005).

information that is being transmitted or abused. Dr. Debarati Halder and Dr. K. Jaishankar go further in formulating a definition of ‘harm’ and they include:

offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim... directly or indirectly, using modern telecommunication networks such as the Internet (networks including but not limited to Chat rooms, emails, notice boards and groups) and mobile phones (Bluetooth/SMS/MMS)’.⁴⁰

This definition would potentially include attempts to falsely impersonate or defame an individual on social media and other public profile websites. Once again, this reopens contentious debates on the extent to which national authorities and courts may (mis)apply or (ab)use criminal law provisions to suppress the freedom of expression and freedom of use of information on the internet. UN Resolutions 55/63 and 56/121 on crushing the criminal abuse of innovation attempted to discover the issue of places of refuge for the individuals who criminally abuse data innovation by mentioning that each nation has made this compelling to lessen the proportion of violations.⁴¹ From that point 2 additional goals were have been received the goals “57/239 and 58/199 on the Creation of a Global Culture of Security and the Protection of Criminal Information Infrastructure.”⁴² The United Nations office is therefore working with its member states to develop a coordination mechanism to effectively address cyberspace related crimes. Pakistan is also a victim of the computer-mediated crimes.

⁴⁰ Debarati Halder & Karuppannan Jaishankar, D. *Cyber Crime and the Victimization of Women: Laws, Rights, and Regulation* (Hershey, PA, USA: IGI Global, 2011).

⁴¹ United Nations General Assembly, “Resolution Adopted by the General Assembly,” 2001,

https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_56_121.pdf

⁴² United Nations General Assembly, “Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures,” 2004, https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf

Pakistan and Digital Violations

Pakistan is a relatively new member of the comity of nations, yet it has outpaced Canada, Spain, Australia. South Korea in online populaces as it is having 47.5 million of web clients operating in the country. In the last four years, Pakistan's online population grew up to 90% after the introduction of 3G and 4G services. However, there is a downside to having more web users in one's country: the more web users, the more digital crimes. So, Pakistan is no exception to cybercrimes. More alarmingly, Pakistan had no adequate cyber laws as late as 2016. Pakistan's parliament passed a cybercrime law in 2016 and this "law envisages 14-year imprisonment and a Rs 5million fine for cyber terrorism, seven-year imprisonment each for campaigning against innocent people on the internet, spreading hate material on the basis of ethnicity, religion, and sect, or taking part in child pornography."⁴³

Moreover, the biggest number of web clients resides cities like Karachi, Islamabad, and Lahore. These three urban areas provide 90% of the client base hence more vulnerable to cybercrimes and online harassment—especially of women.⁴⁴ The use of the internet, in most of the case, is for commercial purposes such as business ventures, demand and supply, and national and individual security, however, its use in identity theft like misrepresentation, provocation, and hacking and cybercrimes is not uncommon either. It was therefore imperative on policy makers to formulate and implement laws for addressing computer-mediated crimes.

⁴³ Geotv, "Cyber Crime Bill Passed in National Assembly," August 11, 2016, <https://www.geo.tv/latest/111200-Controversial-cyber-crime-bill-passed-in-National-Assembly>

⁴⁴ Shirin Naseer & Cameran Ashraf, "Gender-Based Violence in Pakistan's Digital Spaces," *Journal of Feminist Legal Studies*, 30(1) (2022), 29-50.

Cyber-Crime Legislation in Pakistan

Due to fast development in the field of computer and information technology (ICT), Pakistan has a legitimate concern about digital violations. For the first time, Pakistani government issued an ordinance, the Electronic Transaction Ordinance, 2002, for the purpose of documentation, recognition and record keeping, and communication, etc.,⁴⁵ This statute is known as the electronic exchange mandate 2002. The electronic exchange law 2002 is intended to accomplish

1. The greater financial effect.
2. A protected and lawful exchanging occurred between both of the exchanging parties with in the reference to the electronic exchange law 2002
3. Online business and advancing the best Pakistani items like as material, cowhide merchandise, sports products and careful things to the entire world.
4. To expand the E-exchanges
5. Significant advantages for the little and medium business undertakings as the expense of exchanges are enormously diminished electronically.

The Ordinance also “provided for the establishment of an electronic certification accreditation council within 60 days of the promulgation of the ordinance.”⁴⁶ This ordinance considered to be the building bloc of laws related to regulating the cyberspace and to contain cybercrimes.

⁴⁵ Khalid Zafar, “*Electronic Transaction Ordinance, 2002*,” Khalid Zafar & Associates,
<https://khalidzafar.com/laws-of-pakistan/electronic-transaction-ordinance-2002/>

⁴⁶ Dawn, “Electronic Transactions Ordinance promulgated,” September 12, 2002.

Cyber-Crimes Act, 2016

As stated earlier, in august 2016, a significant step towards addressing the cyberspace related issues and challenges in Pakistan, was made when its parliament enacted a law called Prevention of Electronic Crimes Act, 2016. As of 2021, the Federal Investigating Agency (FIA)—Pakistan’s federal agency that deals with cyberspace-related issues—“received a total of 102,356 complaints related to cybercrime in the year 2021. This marks a massive increase in reporting by citizens to the agency tasked for cybercrime under the Prevention of Electronic Crimes Act 2016.”⁴⁷ This is a positive sign as more people now feel confident to report cybercrimes to state officials. However, all was not good with the Act.⁴⁸

The law was liable to be abused and it was abused on several occasion. There is a widespread perception about “digital authoritarian,”⁴⁹ so was the case with the 2016 Pakistani law. This “draconian Prevention of Electronic Crimes Act” was struck down by Athar Minallah, Chief Justice of the Islamabad High Court, in April 2021, by stating:

the criminalization of defamation, protection of individual reputations through arrest and imprisonment and the resultant chilling effect was inconsistent with the Constitution. He further held that the offence under Section 20 of the Prevention of Electronic Crimes Act, 2016, to the extent of the expression ‘or harms the reputation and the punishment thereof is unconstitutional, invalid beyond reasonable doubt and is, therefore, struck down.’⁵⁰

⁴⁷ Usama Khilji, “Rise in Cyber Crimes,” *Dawn* January 11, 2021, <https://www.dawn.com/news/1668802>

⁴⁸ Syed Raza Shah Gilani, Ilyas Khan, and Shehla Zahoor, “The Historical Origins of the Proportionality Doctrine as a Tool of Judicial Review: A Critical Analysis,” *Research Journal of Social Sciences and Economics Review*, 2(1), (2021): 251-58.

⁴⁹ Adrian Shahbaz, “The Rise of Digital Authoritarianism,” *Freedom House*, 2018, https://freedomhouse.org/sites/default/files/2020-02/10192018_Final_Booklet.pdf

⁵⁰ *Dawn*, “Law: A Triumph of Freedom,” April 17, 2022, <https://www.dawn.com/news/1685420>

It is therefore apt to note that there is no denying the fact cyberspace-related crimes are on the rise in the world, but it does not mean that in the garb of preventing such crimes the fundamental rights of individuals are blatantly violated by state authorities.

Recommendations

It is believed that prevention is better than cure, so making and implementing laws would prevent the occurrence of cybercrimes. In addition, creating public awareness will also help in preventing cybercrimes, if not eliminating them altogether. To make that happen, governments must establishment organizations for creating cybercrime awareness; people need to be trained in these organizations about computer-related crimes. State officials must be trained in investigating internet-related crimes. Moreover, regional, and international cooperation is needed to address the problem of identity theft and deception in the “virtual geography.” Lastly, creative solutions involving IT specialists and smart, forward-looking policy makers will help in addressing the problem of digital infringement and to limit the impact of digital wrongdoings— both nationally and internationally.

Conclusion

This article has explored virtual world-related issues such as the definition, patterns and trends in cybercrime and focuses on where does identity theft offences sit in this continuum. In the age of the internet, the integrity, confidentiality, and security of personal data is increasingly at risk. Internet users often exercise little control over how their data is used. These difficulties exist regardless of whether the site of regulation is national, international or business level. Identity theft offenders have shrewdly deployed sophisticated techniques such as phishing to steal personal information. The

personal information obtained is then used to deprive the victims of their valuable assets. It is for this reason that identity crime has been specifically chosen as the focus of this article. Perhaps more than other types of cybercrime, identity theft can only be effectively prevented if data protection and security are addressed together.

Developing countries, often lack the regulatory capacities to effectively address modern crimes like cybercrimes or track down and prosecute individual criminals or networks. Pakistan is one of the countries that may need to revise its cybercrime laws to address these deficiencies, particularly in the areas of data protection and privacy. A priority must be given to strengthen the capabilities of the police and modernize its enforcement strategies and investigating techniques for addressing identity theft and deception. However, the types of identity thefts that have generated most attention in Pakistan, outside the financial arena, are those that have targeted prominent governmental representatives and important state institutions. It is well-nigh impossible to wipe out digital wrongdoing, yet it is conceivable to contain it.



The Third Wave of Democratic Transition in Pakistan: 1988-1990

Muhammad Aslam

*Assistant Professor of Pakistan Studies, Government Ghazali
College & Post Graduate Center Latifabad Hyderabad*

Muhammad Hassan

Senior Research Fellow, NIHCR, QAU, Islamabad

Vol. 4. No. 1/2022

The IJKS

provides a forum for scientific exchange and public dissemination of up-to-date scientific knowledge on the Kashmir conflict, The IJKS is an independent, peer-reviewed, open-access journal.

The topics on which we concentrate—Kashmir conflict and violence—have always been central to various disciplines. Consequently, the journal encompasses contributions from a wide range of disciplines, including international affairs, political studies (geopolitics, political economy and other dynamics, diplomacy and public advocacy, law-based approaches, governance and economy (including micro and macroeconomics), self-determination, and other solidarity rights public international law (including human rights and humanitarian laws and intergovernmental organizations), criminology, economics, education, ethnology, history, political science, psychology, social anthropology, sociology.

All articles are gathered in yearly volumes, identified by a QR Code in print volume with article-wise pagination. For more information, please visit www.kprijk.org

Suggested

APA: Ahmad, I., Ali, Marriam. (2021). Pro-Environment Workforce: Studying Employee Behavior in the Pharmaceutical Companies of at the Sundar Industrial Estate. International Journal of Kashmir Studies, 6.

Citation:

Harvard: Ishtiaq, Ahmad. Marriam Ali. (2021). Pro-Environment Workforce: Studying Employee Behavior in the Pharmaceutical Companies of at the Sundar Industrial Estate International Journal of Kashmir Studies, 6.



This work is licensed under the Creative Commons Attribution-No Derivatives License. ISSN: 2706-5863

The Third Wave of Democratic Transition in Pakistan 1980-1990

Muhammad Aslam

*Assistant Professor of Pakistan Studies, Government Ghazali
College & Post Graduate Center Latifabad, Hyderabad*

Muhammad Hassan

Senior Research Fellow, NIHCR, QAU, Islamabad

Abstract

This research paper tries to explore that how the third wave of democratic transition took place in Pakistan. How the phenomena of democratic transition and consolidation in Pakistan passed through different phases? It also spotlights on the factors which played eminent and effective role for democratic transition as well as consolidation in the country. Moreover, the study explains the process of transition from authoritarianism to democracy in Pakistan while focusing on the theory and practice of transitology and consolidology. The different modes of democratic transition have been discussed to see how democratic transitions in different modes took place in Pakistan. Main concern is to see how different theoretical approaches such as transitology and consolidology are associated in the process of transition from dictatorship to democracy. Political scientists of the world have discussed the democratic transitions that took place in several countries of the world. However, no scholar of this domain from abroad and Pakistan has still investigated that how the third wave of democratic transition took place in Pakistan. In this study, an attempt is made to analyze

transitional history of Pakistan in general and third wave of democratic transition in particular.

Keywords: Pakistan, Democracy, Transition, History and Wave

Introduction

The development of democracy has become a primary concern of the world in the post-cold war era. Before the end of the twentieth century, it was turned into an age of democratic triumph. The global range and influence of democratic ideas, institutions, and practices made that century far and away from the authoritarianism.¹ It was considered as the flourishing period for democracy in human history. In rest of the world particularly in the United States and Europe, after the collapse of the non-democratic systems, the liberal democracy flourished as the final form of human government. In the present era, public considers democracy as the safe system of governance in the World.² In this research paper, the third wave of democratic transitions in the world has been discussed in general and in Pakistan in particular. Main concern is to see how far democracy was consolidated by political leadership of the country.

Since the partition of Sub-continent in the year 1947, Pakistan has entered turbulent process of nation-building. The country's leadership tried to stabilize as well as organized political institutions. Attempts were also made to create harmony among all state actors for the development of people power. Aim was to establish the parliamentary democracy in a well-organized federal setup.³ However, interethnic

¹ B. Talisse Robert, *Democracy after Liberalism: Pragmatism and Deliberative Politics* (New York: Routledge Press, 2005), 1.

² Lauren M. McLaren, *Constructing Democracy in Southern Europe: A Comparative Analysis of Italy, Spain and Turkey* (London and New York: Routledge, 2008), 2.

³ Mahmood Manshipouri and Amjad Samuel, "Development and Democracy in Pakistan: Tenuous or Plausible Nexus?", *Asian Survey*, Vol. 35, No. 11, <http://www.jstor.org/stable/2645722> (Accessed: 12/12/13).

strife, social strains, diverse political ideological background of elites, impacts of praetorian rule and external influence created problems in the nation building process. The fragmented political institutions failed the enforcement of parliamentary democracy in the country.⁴ Philip E. Jones explains that Pakistan often has been its own worst enemy, precipitated into periodic crisis by both blundering generals and overreaching politicians.⁵

The political disaster weakened the roots of democratic foundations in the country. Instead of promoting the tradition of civilian supremacy bequeathed by Great Britain, the civilian rulers have often relied on the military to preserve their vested power.⁶ The self-interests and policies of civilian politicians also destroyed the equilibrium of political institutions in Pakistan. It paved the ways for dictators for intervening in the politics of the country.⁷ However, its political culture and civil society remained rich in the creation of many people of integrity, principles and coherent political vision; a few of them like Zulfikar Ali Bhutto and his daughter Benazir Bhutto have risen to national power.⁸

Despite transitions from dictatorships to democracies from time to time and steps taken by political leadership (Bhutto and Muhammad Khan Junejo) in distancing military from politics of the country could not prevent other military coups in Pakistan.⁹ The reason was dictatorial attitude and anti-democratic behaviour of politicians. In fact, there was dire need of pro-democracy environment. However,

⁴ Veena Kukreja, *Contemporary Pakistan Political Process, Conflicts and Crisis* (New Delhi: Sage Publications, 2003), 16.

⁵ Philip E. Jones, *The Pakistan People's Party: Rise to Power* (Oxford University Press, 2003), 1.

⁶ Manshipouri and Samuel, "Development and Democracy in Pakistan: Tenuous or Plausible Nexus?"

⁷ Kukreja, *Contemporary Pakistan Political Process*, 17.

⁸ Jones, *The Pakistan People's Party*, 5.

⁹ Kukreja, *Contemporary Pakistan Political Process*, 18.

vested-political interests and anti-democratic policies of political parties consolidated authoritarian political culture in the country.¹⁰ The vision followed by political leadership was complicated. Thus, it provided space to generals to intervene the political institution of the country.

A Brief Transitional History of Pakistan

General Ayub imposed first martial law in Pakistan on October 7, 1958 in Pakistan. However, no organized movement was launched against unconstitutional government of Ayub Khan's martial law.¹¹ After almost a decade, in the year 1967, political parties such as Awami Muslim League, Council Muslim League, Nizam-i-Islami Party and Jamat-i-Islami established Pakistan Democratic Movement (PDM).¹² The struggle of political parties resulted in transition from dictatorship to democracy in Pakistan.¹³ During this era, the first wave of democratic transition was in progress in the world.

After a half decade, Pakistan National Alliance (PNA) opposed Bhutto government and they launched movement for the removal of Bhutto in the year 1977.¹⁴ Moreover, it was a union of heterogeneous political parties (i) Tehrik-i-Istaqlal (TI) (ii) Jamaat-i-Islami (JI) (iii) Jamiatul-Ulma-e-Islam (JUI) (iv) Jamiatul Ulema-e-Pakistan (JUP) (v) Muslim League Pagaro Group (PML Pagaro) (vi) National Democratic Party (NDP) (vii) Pakistan Democratic Party (PDP) (viii) Khaksar Tahreek (KT) (ix) Azad Kashmir Muslim Conference

¹⁰ Saeed Shafqat, "Democracy in Pakistan: Value Change and Challenges of Institution Building", *The Pakistan Review*, Vol. 37, No. 4, <http://www.jstor.org/stable/41261058> (Accessed: 11/12/2013 02:32).

¹¹ Stanley Wolpert, *Zulfi Bhutto of Pakistan: His life and Times* (New York: Oxford University Press, 1993), 209.

¹² *The Pakistan Times*, May 2, 1967.

¹³ Wolpert, *Zulfi Bhutto of Pakistan*.

¹⁴ *The Dawn*, January 12, 1977.

(AKMC).¹⁵ The PNA launched a movement against elections of 1977 and demanded fresh elections. The movement against mal-practices in the elections resulted in chaos which resulted in imposition of Martial Law by the then army chief, General Zia Ul Haq.¹⁶

The Pakistan Peoples' Party formed an alliance with Pakistan Democratic Party (PDP), Tehrik-i-Istiqlal (TI), Pakistan Muslim League (Khawaja Khariuddin Qasim group), Quami Mahaz-i-Azadi (QMA), Mazdoor Kisan Party, Jamiat-i-Ulema-i-Islam and Kashmir Muslim Conference (KMC) launched opposition movement for the restoration of democracy in Pakistan on February 6, 1981.¹⁷ They name it MRD (Movement for the Restoration of Democracy). They desired transition from dictatorship to democracy in Pakistan.¹⁸ During this period, the era of third wave of democratic transition had already taken place in the world.

In analyzing democratic transitions in recent years, social and political scientists have distinguished between problems of "transitions from authoritarian rule" and problems of "democratic consolidation."¹⁹ In this research paper, the factors are focused that how an authoritarian regime can be suppressed and how democracy can flourish in Pakistan. The paper has briefly spotlighted the historical background of democratic transition in the World to develop comparative thoughts on the democratic transition in case of Pakistan. It has also tried to bring theories of democratic transition

¹⁵ Hassan Askari Rizvi, *Military, State and Society in Pakistan* (London: Macmillan Press Ltd, 2000), 223.

¹⁶ *The Dawn*, July 06, 1977.

¹⁷ Farkhanda Bukhari, *Ye Bazi Ishq ki Bazi hai (It is the Matter of Intense Love)* (Lahore: Sang-i-Meel Publications, 2012), 65-66.

¹⁸ Faiz Khoso, *Kare Kakkar Heth Mu Jharrendea Chaddiya: Tarikhee Halchal MRD (Fighting Sprit under Dark Cloud: Historical Movement MRD)* (Hyderabad: My Publications, 2013), 11.

¹⁹ Irving Leonard Markowitz, *Constitutions, the Federalist Papers, and the Transition to Democracy*, ed: Lisa Anderson, *Transitions to Democracy*. (New York: Columbia University Press, 1999), 45.

and consolidation. Main concern is to see a connection of theory and practice of democratic transition and consolidation in case of Pakistan.

The Third Wave of Democratic Transition in the World

The term transition is defined as the change from one state to another state (From democracy to dictatorship or authoritarianism to people's rule and from civilian government to military regime). Transition may occur due to crisis and it may also take place without any crisis.²⁰ The six crisis transitions include Argentina, Bolivia, Uruguay, the Philippines, Brazil and Peru. In Argentina, Bolivia, Uruguay, and the Philippines, regime transitions took place during deep recessions and crisis. In four countries such as Chile, Korea, Thailand and Turkey transition occurred without crisis.²¹ In these countries authoritarian rulers left the offices due to pressure from international and domestic forces.²²

In the recent years, transition has taken place in the number of countries where political institutions were occupied by unelected regimes including military, one-party or non-party and personalist dictatorships. This political occupation took place before the emergence of democracy. A sea of change has taken place in Latin American politics. In most of the region, until the waves of democratization that started in 1974, authoritarian regimes were pervasive.²³ As far as wave of democracy is concerned, it is said to have started in Southern Europe in the mid-1970s, before spreading to Asia. Eventually the result was that, whereas in the early 1970s,

²⁰ Talisse, Democracy after liberalism, 1.

²¹ Dankwart A. Rustow, Transitions to Democracy: Toward a Dynamic Model Lisa Anderson, ed: Lisa Anderson, *Transition to Democracy*, 79.

²² Jon Elster, *Retribution and Reparation in the Transition to Democracy* (New York: Cambridge University Press, 2006), 3.

²³ Sylvia Chan, *Liberalism, Democracy and Development* (United Kingdom: Cambridge University Press, 2004), 14.

only a quarter of countries had democratically elected governments, two decades later more than 50 percent had adopted this system. By the end of the 1990s, about 75 percent of governments around the world were elected.²⁴

Many Asian countries have also gone through a period of developmental dictatorship in the 1960s and 1970s such as Pakistan, Burma and Philippines. However, most of these dictatorships broke up in the 1980s and thereafter a new period of post-dictatorship era opened. This post-dictatorship era was known as period of 'democratic transition', 'democratic consolidation' or democratization broadly.²⁵ The political circumstances have firmly altered.²⁶ Many countries were facing social and economic problems during that era.²⁷ In Argentina and Brazil, democratic government withstood annual inflation rates that went far into quadruple digits. In El Salvador and Guatemala, countries with histories of brutal authoritarianisms, consistent repression of the indigenous populations, and horrendous civil wars, warring factions signed peace treaties and established elected regimes.²⁸

Theoretical Framework: The Modes of Transition

The term transition covers different modes and stages. The parameters and standards of transition depend on the political culture which varies from country to country. Apart from this, the nature of transition also varies from country to country. Transitions include gradual change, as the authoritarian regime and the opposition engage

²⁴ Jeff Haynes, *Democracy and Political Change in the Third World* (New York: Routledge Press, 2001), 1.

²⁵ Samuel P. Huntington, *The Third Wave: Democratization in the Late Twentieth Century* (Oklahoma: University of Oklahoma Press, 1991), 13.

²⁶ Haynes, *Democracy and Political Change in the Third World*.

²⁷ Talisse, *Democracy after Liberalism*, 6.

²⁸ Chan, *Liberalism, Democracy and Development*, 15.

in a long bargaining process.²⁹ Or transitions can be the outcome of rapid dramatic ruptures in the balance of power between the regime and the opposition.³⁰ Samuel P. Huntington developed three major modes of transition with substantial examples such as Transformation, Trans placement and Replacement.³¹

(a)Transformation

In the phenomenon of transformation, when transition from dictatorship to democracy is supposed to begin, the authoritarian ruler acts alone more actively or less actively to defend his unconstitutional rule. The stakeholders of dictatorial rule play main role in the conversion of authoritarianism into democratization.³² This mode of transition is enduring and longtime taking phenomenon that takes place when an authoritarian rule, except reasonable pressure generated by opponents of authoritarianism or political forces and other social elements of the society does not leave the office. The political pressure generated by pro-democracy may be supportive for political change and national interest.³³

Transformation usually takes place in well-established military regimes, where ultimate means of coercion are under the control of economically successful governments.³⁴ This mode of transition is slow and gradual. It also gives better outcomes to ouster military out of the political arena.³⁵ In simple words, the result of transformation

²⁹ Chan, *Liberalism, Democracy and Development*, 17.

³⁰ Gretchen Casper and Michelle M. Taylor, *Negotiating Democracy: Transitions from Authoritarian Rule* (Pittsburgh: University of Pittsburgh Press, 1996), 5.

³¹ Huntington, *The Third Wave*, 124.

³² Jeff Haynes, *Democracy in the developing World: Africa, Asia, Latin America and the Middle East* (USA: Polity Press, 2001), 24.

³³ Gerardo L. Munk, *Measuring Democracy: A Bridge between Scholarship and Politics*. (America: The Johns Hopkins University Press, 2009), xi.

³⁴ Huntington, *The Third Wave*, 125.

³⁵ Chan, *Liberalism, Democracy and Development*, 15.

is likely to be, at best, a limited democracy notable for the continued political dominance of relatively small number of elite apparatus.³⁶

(b) Transplacement

In the process of transplacement, transition from dictatorship to democracy occurs through the mutual actions of the opposition and government. The transition is possible through the negotiations among the elites both in the power and beyond the power.³⁷ The commitment among elites for democratization is necessary provision for political change.³⁸ Moreover, Linz and Stephan explain that commitment of political leadership and elites is of the vital significance.³⁹ In other words, the conceptual framework of this mode of transition depends on the harmony among the political leadership and elites.

Approximately, eleven of thirty-five liberalizations and democratizations occurred in the 1970s and 1980s by the process of transplacement.⁴⁰ Initially, both the forces such as government and opposition try to suppress each other's strength and unity. With the passage of time, both government and opposition realize that the workable plan only be chalked out through negotiations and both the forces decide to forget the past and begin negotiations to settle the turmoil what Huntington calls trans placement.⁴¹

In this whole phenomenon, stakeholders in power such as older military officials, elites within opposition as well as government and large-scale feudal lords are not disturbed. Their power is not jeopardized in the new order (political setup). Haynes notes how

³⁶ Haynes, *Democracy in the developing World*, 25.

³⁷ Stepan, *Problems of Democratic Transition and Consolidation*.

³⁸ Haynes, *Democracy in the Developing World*, 27.

³⁹ Stepan, *Problems of Democratic Transition and Consolidation*.

⁴⁰ Haynes, *Democracy in the Developing World*, 151.

⁴¹ Huntington, *The Third Wave*, 152.

imperative it is for political stability after the transition to integrate elite into stable political democratic setup that does not destroy their interests. However, elites do not judge that their interests are protected in the new stable democratic setup.⁴²

(c) Replacement

Replacement is the major mode of transition which differs from transformation and transplacement. Replacement needs imperatives such as severe national crisis and inability of government. It also takes place when government faces problems and opposition become more power than government.⁴³ The former opposition groups replace government and they come to power. Moreover, they often enter a new phase as groups in the new government covers three distinct phases: the struggle to produce the fall, the fall, and the struggle after the fall.⁴⁴ The phenomenon of replacement does not require the elite settlement and their dominance. However, this phenomenon increases pressure against elites to leave the office and accept the will of public.

In this mode of transition, authoritarian rule is mostly ousted out of the power structure by mass mobilization. However, it does necessarily not replace authoritarian regime with democratic regime. In the replacement process, it is also possible that authoritarian regime may be occupied by another type of authoritarian rule.⁴⁵ As was the case in Pakistan, after prolonging protests, demonstrations, marches, strikes, rallies and processions, General Ayub Khan's enduring dictatorial rule was replaced by another military dictator General Yahya Khan. This happened due to absence of harmony and mutual understanding among the leadership of democratic forces. It also results in the creation of hindrance to the emergence of the necessary

⁴² Haynes, *Democracy in the Developing World*, 23-25.

⁴³ Stepan, *Problems of Democratic Transition and Consolidation*.

⁴⁴ Huntington, *The Third Wave*, 142.

⁴⁵ Haynes, *Democracy and Political Change in the Third World*.

climate of moderation and compromise characterizing democratic consolidation.⁴⁶ In transformations and transplacements, the stakeholders in the authoritarian regime usually leave the politics and return to the barracks or private life quietly and with some honour and dignity. At times, authoritarian regimes are ousted out of power through replacement mode of transition.⁴⁷

Transition is an interesting and an excited phenomenon particularly in context to the countries whose political system is weak, ideologically fragmented, and nationally disintegrated.⁴⁸ Dank Wart A. Rustow's article 'Transition to Democracy' is appeared to be a dynamic model which explains important problems of transition at the time.⁴⁹ In the light of problems in political cultures of different countries, he explains that the consolidation of democracy passes through different stages. In this research article, it is to discuss how democratic transition and consolidation crossed these five stages in the case of Pakistan.

Democratic Transition and Consolidation in Pakistan

The first stage of democratic consolidation requires national unity and stability. The development of national unity is necessary to consolidate democracy in political system of polity.⁵⁰ Unfortunately, national unity could not be achieved in Pakistan since partition. Incomplete partition of United India into two countries Pakistan and India by British created international problems in the region such as Kashmir dispute and water problem.⁵¹

⁴⁶ Haynes, *Democracy in the Developing World*, 27.

⁴⁷ Huntington, *The Third Wave*, 152.

⁴⁸ Munk, *Measuring Democracy*.

⁴⁹ Dankwart A. Rustow, "Transitions to Democracy: Toward a Dynamic Model Lisa Anderson," ed: Lisa Anderson, *Transition to Democracy*, 79.

⁵⁰ Haynes, *Democracy in the Developing World*, 25.

⁵¹ Ian Talbot, *Pakistan: A Modern History* (London: Hurst & Company, 1988).

In the second stage, mass movements and public unity are necessary provisions for the development of democracy. In this phase of democratic consolidation, polity goes through a prolonged and inclusive political struggle. After transition from dictatorship to democracy, the democratic consolidation may be the result of long lasted mass movement.⁵² In simple words, this stage is dependent on the intense political struggles and movements. In the case of Pakistan, MRD's (Movement for the Restoration of Democracy) ⁵³ struggle to bring Pakistan on the road of democracy was not successful but it developed pressure on dictator Zia for democratic transition in the country.⁵⁴ Post MRD era, the democratic transition took place in Pakistan through regime rupture. Resultantly, people's rule was established in 1988 and steps were taken to consolidate democracy in the country.⁵⁵ Due to lack of political harmony as well as diverse political ideologies resulted in transition from democracy to dictatorship for the third time in Pakistan on October 12, 1999.⁵⁶

The third stage of transition is signifier of compromises among competitors such as dictators versus dictators and democrats versus democrats; therefore, this stage is called as the inception of transition⁵⁷ because leading political players decide to compromise, to adopt democratic rules and create unity. In this phase, political leaders usually work according to democratic rules for the consolidation of democracy.⁵⁸ Moreover, this stage is mainly associated with the politics of reconciliation.⁵⁹ During Musharraf era,

⁵² Haynes, *Democracy and Political Change in the Third World*

⁵³ Muhammad Waseem, *Pakistan Under Martial Law 1977-1985* (Lahore: Vanguard Book (Pvt) ltd., 1987).

⁵⁴ Talbot, *Pakistan*.

⁵⁵ Mushahid Husain, *Pakistan's Politics: The Zia Years* (Lahore Progressive Publishers, 1990).

⁵⁶ Aqil Shah, *The Army and Democracy: Military Politics in Pakistan* (London: Harvard University Press, 2014).

⁵⁷ Munk, *Measuring Democracy*.

⁵⁸ Haynes, *Democracy in the Developing World*, 2 9.

⁵⁹ Husain, *Pakistan's Politics*.

the and the then Co-chairman of PPP, Asif Ali Zardari reconciled politically with opposition for the consolidation democracy in the country.⁶⁰

The fourth stage is called as the second transition in which democratic construction and consolidation begin to become mature.⁶¹ the contemporary phase of the history of Pakistan can be called the era of consolidation of democracy with certain complexities and uncertainty. In countries like Pakistan, the development and empowerment of democracy remain non-permanent. As a result, authoritarianism easily finds its roots to flourish in the political system of the countries like Pakistan.⁶² The history reveals in Pakistan that democratic transition and consolidation processes have been passing these all stages since the inception of the partition era. However, no pro-democracy atmosphere has yet been created in Pakistan.⁶³

Dynamics of Democratic Consolidation in Pakistan

The circumstances and factors that are concerned with democratic consolidation are spotlighted here including vastly consensual, political attitude, social structures and political institutions.⁶⁴ There are other eminent factors regarding democratic consolidation such as level of national prosperity; a robust relatively well-organized civil society; and an institutionalization, relatively undivided as well as political party system.⁶⁵ There are also converse factors that prevent

⁶⁰ Faiz Khoso, *Kare Kakkar Heth Mu Jharrendea Chaddiya: Tarikhee Halchal MRD (Fighting Sprit under Dark Cloud: Historical Movement MRD)* (Hyderabad: My Publications, 2013), 11.

⁶¹ Haynes, *Democracy in the Developing World*, 30.

⁶² Lawrence Ziring, *Pakistan at Cross Currents of History* (Lahore: Vanguard Books, 2004).

⁶³ Ian Talbot, *Pakistan: A Modern History* (London: Hurst & Company, 1988).

⁶⁴ Robert. B. Talisse, *Democracy After liberalism: Pragmatism and Deliberative Politics*, 102.

⁶⁵ Munk, *Measuring Democracy*.

democratic consolidation enduring economic crisis, lack of societal toleration among ethnically and or religiously divided groups; a weak civil society; a highly fragmented party system; factional party politics.⁶⁶

Among the Muslim states and developing world, Pakistan is one of those a few states, where people prefer parliamentary democratic system and have shown their strength to reject military dictatorships through mass movements and mobilization.⁶⁷ The upsurge of mass movements for the revival of democracy such as PDM (Pakistan Democratic Movement, Anti-Ayub Movement, MRD and ARD (Alliances for the restoration of Democracy) showed the disapproval of military rule in Pakistan.⁶⁸ Non-serious attitude of politicians could not produce healthy atmosphere for the promotion of stable democracy in the country.⁶⁹

Democracy in Pakistan, rather emerged by default once the ruling regime voluntarily stepped aside after the sudden death of General Zia and his top brass in plane crash on August 17, 1988.⁷⁰ From 1988 to 1999 Benazir Bhutto and Nawaz Sharif emerged to represent new generation. Both the political leaders from different political parties took steps in their own patterns to consolidate democracy and uphold rule of law. They began political retaliation rather than following democratic rules. But both applied conceptual framework of autocratic tendencies that gave birth to the politics of retaliation. The challenges for the party leadership in Pakistan are to transform the

⁶⁶ Huntington, *The Third Wave*, 155.

⁶⁷ Rasool B. Rais, "Elections in Pakistan: is Democracy Winning?," *Asian Affairs*, Vol. 12, No. 03, (Spring, 1988): 78-97.

⁶⁸ Tarique Ali, "Movement for the Restoration of Democracy in Pakistan," *India International Centre Quarterly*, Vol. 11, No. 01, (March 1984): 57-79.

⁶⁹ Shafqat, "Democracy in Pakistan: Value Change and Challenges of Institution Building".

⁷⁰ C.G.P. Rakisits, "Centre-Province Relations in Pakistan Under President Zia: The Government's and Opposition's Approaches," *Pacific Affairs*, Vol. 61, No. 1, (Spring, 1988): 78-97.

character of political party from an instrument of mass mobilization to interest representation and advocacy in the parliament. In the political history of Pakistan an outstanding feature in party politics has been the construction and tearing of alliances and coalitions.⁷¹ However coalitions are proved to be weak within the parliament but in rare cases multiparty consensus on issues developed. The best example is the removal of the eighth amendment.

In fact, democracy was never allowed to flourish in political atmosphere of Pakistan. The fact of irony is that political culture of Pakistan is dependent on several classes and sub-classes which include fragmented civil society in the form of bridaries, feudal communities, and fragmented political party system. In such political system, when champions of democracy, who struggled and desired to bring the country on the routes of democracy. They are not only suppressed but also ousted out of the political arena by several anti-democratic forces.⁷²

In spite of movements and a huge struggle for the restoration of democracy in Pakistan, the political leadership of Pakistan People's Party has been unable to formulate a legal frame and most eminently neither built a network of policies nor gave birth to a pro-democratic environment in which contradictions among political elites may be solved. But they have only developed a framework on the basis of reconciliation for the consolidation of their own positions. The promotion and progress of democracy require patience, consensus, political dialogue and deliberation among the powerful groups and political parties. Democracy cannot function vigorously in the absence of elite consensus and harmony.

⁷¹ Shafqat, "Democracy in Pakistan: Value Change and Challenges of Institution Building".

⁷² Khalid Bin Saeed, "Pakistan in 1983: Internal Stresses More Serious than External Problem," *Asian Survey*, Vol. 24, No. 02, (February 1984): 219-28.

Conclusion

This research article concludes in the light of theoretical framework that transitions from democracy to dictatorship take place either by regime rupture, elite settlement, social, economic and political crisis as well as mass mobilization. Ayub Khan left office due to political crisis and mass mobilization against his regime. Yahya Khan transferred powers to civilians after election process (elite settlement). General Zia's downfall became by disaster (his death in plane crash). However, crisis did not remain the main cause of democratic transition in Pakistan. Despite restoration of democracy, political leadership faced failure to consolidate democracy and develop healthy atmosphere for democracy in Pakistan. Their vested interests and dictatorial autocratic attitude weakened democracy in the country. Therefore, the process of democratic consolidation remained slow and democracy did not lay its foundation roots to nourish in Pakistani state. Finally, this research paper concludes that democracy could be promoted in future. If political leadership could either change their autocratic attitude or follow the principles of democracy. By doing this, healthy democratic atmosphere could be developed in Pakistan.

Call for Papers

The International Journal of Kashmir Studies (IJKS) invites the submission of articles and book reviews for the next of this journal. It's a peer reviewed bi-annual journal confronting to the standards of HEC recognize journal and aspire to be soon recognized by HEC. We invite submissions form academics and PhD candidates, diplomats, decision-makers and activists. IJKS accepts scholarly work encompassing (but not limited to) the research themes relating Kashmir conflict such as:

- International Affairs (relations/linkages)
- Political Studies (Geopolitics, Political Economy and other dynamics)
- Diplomacy and Public Advocacy
- Security Paradigm
- Defense and Strategic Studies
- Law based Approaches
- Peace and Conflict Studies (in the perspectives of History, Sociology, Anthropology, Psychology, Art, Culture, Archeology, Heritage, Religion, Development, Business, Trade, Commerce, Languages, Disaster Management, Climate, Environment, Geography Media and Mass Communication and Education etc.)
- Governance and Economy (including micro and macroeconomics)
- Self-determination and other solidarity rights Public International Law (including human rights and humanitarian laws and intergovernmental organizations)

Please refer to submission guidelines <http://kprijk.org/instructions-for-authors/> as articles not following this format will not be considered.

We look forward to receiving your manuscript so it can be considered. To submit articles, please contact us at chiefeditorijks@kprijk.org with the title: "IJKS Articles Submission".