Digital Authoritarianism and Activism for Digital Rights in Pakistan

ZAHID SHAHAB AHMED
IHSAN YILMAZ
SHAHRAM AKBARZADEH
GALIB BASHIROV

JULY 20, 2023

DOI.ORG/10.55271/rp0042
BIOS

**DR. ZAHID SHAHAB AHMED** is a Senior Research Fellow at Alfred Deakin Institute for Citizenship and Globalization, Deakin University, Australia. He is also a Non-Resident Research Fellow at the Institute of South Asian Studies, National University of Singapore. During 2017-19, Dr Ahmed was a Non-Resident Research Fellow with the University of Southern California's Center on Public Diplomacy. During 2013-16, he was an Assistant Professor at the Centre for International Peace and Stability, National University of Sciences and Technology in Pakistan. His work focuses on political developments (e.g., democratization, authoritarianism and political Islam), foreign affairs, peace and security in South Asia and the Middle East. He has published extensively in leading journals, such as Politics and Religion, Democratization, Asian Studies Review, and Territory, Politics, Governance. He is the author of Regionalism and Regional Security in South Asia: The Role of SAARC (Routledge, 2013). He is a co-author of Iran's Soft Power in Afghanistan and Pakistan (Edinburgh University Press, 2023). Email: zahid.ahmed@deakin.edu.au

**IHSAN YILMAZ** is Research Professor and Chair of Islamic Studies and Intercultural Dialogue at the Alfred Deakin Institute for Citizenship and Globalization (ADI), Deakin University, Melbourne, Australia. He has conducted research on nation-building; citizenship; ethnic-religious-political identities and their securitization (Middle East, Pakistan, Indonesia); minority-majority relations (Australia, Turkey, the UK, and the USA); socio-legal affairs, identities, belonging and political participation of Muslim minorities in the West (the UK, Australia, and the USA); Islam-state-society relations in the majority and minority contexts; global Islamic movements; political Islam in a comparative perspective; Turkish politics; authoritarianization; Turkish diasporas (the UK, Australia, the USA); transnationalism; intergroup contact (Australia); and politics of victimhood (Australia, Turkey).

**DR. SHAHRAM AKBARZADEH** is Convenor of Middle East Studies Forum (MESF) and Deputy Director (International) of the Alfred Deakin Institute for Citizenship and Globalisation, Deakin University (Australia). He held a prestigious ARC Future Fellowship (2013-2016) on the Role of Islam in Iran’s Foreign Policy-making and recently completed a Qatar Foundation project on Sectarianism in the Middle East. Prof Akbarzadeh has an extensive publication record and has contributed to the public debate on the political processes in the Middle East, regional rivalry and Islamic militancy. In 2022 he joined Middle East Council on Global Affairs as a Non-resident Senior Fellow. Google Scholar profile: https://scholar.google.com.au/citations?hl=en&user=8p1PrpUAAAAJ&view_op=list_works Twitter: @S_Akbarzadeh Email: shahram.akbarzadeh@deakin.edu.au

**DR. GALIB BASHIROV** is an associate research fellow at Alfred Deakin Institute for Citizenship and Globalization, Deakin University, Australia. His research examines state-society relations in the Muslim world and US foreign policy in the Middle East and Central Asia. His previous works have been published in Review of International Political Economy, Democratization, and Third World Quarterly. Google Scholar profile: https://scholar.google.com/citations?user=qOt3Zm4AAAAJ&hl=en&oi=ao Email: galib.bashirov@deakin.edu.au

**Funding:** This research was funded by Gerda Henkel Foundation, AZ 01/TG/21, Emerging Digital Technologies and the Future of Democracy in the Muslim World.
EXECUTIVE SUMMARY

With the Pakistani government implementing rules and regulations to control the online sphere, particularly through the Prevention of Electronic Crimes Act (PECA), digital authoritarianism has emerged as a significant governance tool in the country. Concerns have been raised regarding potential abuses stemming from the vague definitions of cybercrime within PECA and the extensive monitoring authority granted to intelligence services. However, despite the rise of digital authoritarianism, a countervailing force exists. Pakistan’s judiciary has displayed resistance, and the nation boasts a robust civil society that includes human rights organizations focusing on digital rights. These groups express concerns regarding data security, privacy regulations, and the internet access of marginalized communities. This study aims to examine the dynamics of digital authoritarianism in Pakistan and evaluate the role of civil society organizations in promoting and protecting digital rights.

Initially, communications in Pakistan were governed by colonial-era legislation, such as the Pakistan Telecommunication (Re-organization) Act of 1996 and the Telegraph Act of 1885. The Fair Trial Act of 2013 enabled the extensive collection of evidence through monitoring. These regulations, coupled with the absence of a comprehensive digital governance bill, have facilitated continuous online surveillance. Pakistan has witnessed remarkable growth in internet penetration, with approximately one-third of the population now having internet access.

In 2016, Pakistan introduced the Prevention of Electronic Crimes Act (PECA) to address internet governance. The act imposes severe penalties for various offences, including hacking, cyberstalking, and cyberterrorism. However, concerns have been raised regarding issues such as misuse, limitations on expressive rights, and privacy violations. PECA grants increased authority to institutions like the Pakistan Telecommunication Authority (PTA) and the Federal Investigation Agency (FIA) for digital surveillance and prosecution. The PTA possesses extensive powers to block and remove content, often justifying these actions based on the grounds of promoting vulgarity or corrupting the youth. Social media companies are also required to comply with specific regulations.

Pakistan benefits from a strong network of civil society organizations that actively collaborate with international counterparts to raise awareness about digital rights. Within Pakistan, several prominent organizations are dedicated to advocating for digital rights, internet freedom, privacy, and digital literacy.

The Digital Rights Foundation is a notable non-profit organization that focuses on promoting digital rights and addressing issues such as online harassment, data security, freedom of speech, and women’s digital rights. They conduct research, provide legal support, and deliver training and awareness programs on digital security.

Bolo Bhi is another civil society organization committed to
internet freedom, digital security, and open access to information. Alongside policy advocacy, research, and digital literacy initiatives, they raise public awareness about internet censorship, surveillance, and privacy concerns.

Media Matters for Democracy is a group that works on freedom of expression, digital rights, and media development in Pakistan. Through research, policy advocacy, and capacity-building initiatives, they strive to enhance online civic spaces, promote digital literacy, and safeguard digital rights.

The Internet Policy Observatory Pakistan, a research project, offers policy recommendations on issues such as data privacy, monitoring, and censorship. They track and analyse internet governance challenges in Pakistan.

Privacy International, a global organization, advocates for privacy rights and opposes intrusive monitoring practices, including in Pakistan.

These civil society organizations play crucial roles in promoting and safeguarding digital rights in Pakistan, both through local advocacy efforts and international collaborations. These organizations actively engage in research, lobbying, and capacity-building initiatives to interact with politicians, raise public awareness, and protect digital rights in Pakistan. They also address the issue of inadequate internet access, particularly in rural and underserved areas. Their initiatives serve as a reminder of the significance of inclusive policies, digital literacy programs, bridging the digital divide, and ensuring that technological advancements are guided by human rights principles.

By conducting research, these organizations generate valuable insights into the challenges and opportunities related to digital rights in Pakistan. They utilize this research to advocate for policies that protect individuals’ online freedoms and privacy. Through lobbying efforts, they aim to influence policymakers and lawmakers, urging them to enact laws and regulations that promote digital rights and address concerns regarding internet access, privacy, and surveillance. Capacity-building initiatives undertaken by these organizations involve educating individuals and communities about digital rights, empowering them to understand their rights and navigate the online world safely. These efforts are particularly vital in rural and underserved areas, where access to information and digital literacy may be limited.

The organizations’ commitment to addressing the digital divide highlights the importance of ensuring equal and affordable internet access for all citizens, regardless of their geographical location or socioeconomic status. Furthermore, these organizations emphasize the need for human rights principles to underpin technological advancements. They advocate for a responsible and ethical approach to digital development, wherein individual privacy, freedom of expression, and other fundamental rights are respected and protected.
POLICY IMPLICATIONS

– The ambiguous definitions of cybercrime within the Prevention of Electronic Crimes Act (PECA) give rise to concerns regarding potential abuses and violations of privacy. To address these issues and ensure the protection of individual rights, it is imperative for the government to undertake a thorough review and modification of the Act. This review should involve establishing precise definitions for cybercrimes and implementing stringent regulations governing the collection, storage, and utilization of personal data. Additionally, robust data protection laws need to be put in place to safeguard the privacy of individuals.

– Given the wide-ranging monitoring authority granted to intelligence services under PECA, there is a pressing need for stronger supervision and accountability mechanisms. To prevent the potential abuse of surveillance powers and protect individual rights, it is crucial to establish independent authorities tasked with overseeing and regulating the operations of intelligence services. Transparency and accountability should be prioritized through regular audits and reporting procedures, ensuring that the actions of these services align with legal and ethical standards. By implementing robust oversight measures, we can safeguard against potential abuses and maintain the balance between security concerns and individual privacy rights.

– The resilience displayed by the judiciary in Pakistan against digital authoritarianism is commendable. However, there is still room for improvement in terms of enhancing judicial independence and equipping courts with the necessary tools to effectively address matters related to digital rights. To enhance the judiciary’s understanding of the complexities involved, it is crucial to implement judicial training programs focused on technology and digital issues. These training initiatives can provide judges with the knowledge and skills needed to navigate the intricacies of digital matters and make informed decisions. By bolstering judicial comprehension in this field, the judiciary’s ability to uphold and protect digital rights in Pakistan can be strengthened.

– The government should prioritize initiatives aimed at closing the digital divide and improving internet access, especially in rural and underserved areas. This requires making substantial investments in infrastructure development, expanding broadband availability, and reducing internet service costs. Additionally, implementing digital literacy programs is crucial to equip individuals with the necessary skills to navigate the digital realm securely and effectively. By addressing these issues, the government can empower marginalized communities, bridge the digital gap, and create equal opportunities for all citizens to participate in the digital age.

– Civil society groups in Pakistan are at the forefront of promoting digital rights. Recognizing their expertise and advocacy efforts, the government should actively
engage with these organizations and seek their advice and insights in formulating rules and regulations. Collaborating with civil society groups allows for a comprehensive and inclusive approach to addressing the diverse issues and viewpoints related to digital rights. By fostering meaningful dialogue and incorporating the perspectives of various stakeholders, the government can develop more effective policies that uphold and protect digital rights in Pakistan.

– Extensive public awareness campaigns are essential to educate the public about their digital rights, emphasizing the importance of online privacy and security. These awareness efforts should be inclusive, targeting various social groups, with a particular focus on marginalized communities. The aim is to equip individuals with the knowledge and skills to protect their personal information online, recognize potential risks, and take appropriate legal action if their rights are violated. By empowering people with this information, we can foster a safer and more informed digital environment, ensuring that individuals are aware of their rights and can actively safeguard their online privacy and security.

– Pakistan should actively engage in international forums and collaborate with other nations to establish best practices and standards in addressing digital rights issues, recognizing the global nature of these challenges. By participating in these forums, Pakistan can benefit from shared knowledge and experiences, leading to more effective approaches in protecting digital rights. Collaborating with organizations like Privacy International can be instrumental in leveraging their expertise and assistance to strengthen privacy rights and oppose intrusive surveillance practices. By working together on an international scale, Pakistan can contribute to the development of robust frameworks for digital rights protection and ensure that privacy and individual freedoms are upheld in the digital realm.
Pakistan’s political landscape has been profoundly shaped by its historical trajectory, which has been marred by violence, religious divisions, and an intricate struggle for identity. The country has faced challenges in establishing a stable democracy, with periods of military dictatorship undermining democratic processes. Governance issues, such as limited freedom of the press, restricted right to protest, and interference from the military establishment, have cast a shadow on Pakistan’s democratic credentials. Furthermore, the rise of digital authoritarianism has added a new dimension to the country’s political landscape.

To govern the digital sphere, the government has implemented laws and regulations, with the Prevention of Electronic Crimes Act (PECA) serving as foundational legislation. However, concerns arise from the ambiguous definitions of cybercrime in PECA, and the extensive surveillance powers granted to civil and military intelligence agencies, raising the potential for abuse of power. The state has invested in technological capabilities for online monitoring, including web monitoring systems and social media monitoring cells. This digital surveillance infrastructure, combined with the expanded role of state institutions, reinforces the government’s control over cyberspace and its citizens’ privacy.

While digital authoritarianism is on the rise, characterized by increased surveillance, internet shutdowns, and
Pakistan as a young nation-state. Despite being a ‘Muslim’ state, Pakistan at the time of its creation hosted a 23 percent population of non-Muslims, which has dwindled to 4 percent at present, and newly independent India did and still houses millions of Muslims (Mehfooz, 2021). Adding to this, the 1971 civil war led to the separation of East Pakistan from the union resulting in the creation of Bangladesh (Hossain, 2021, 2018). This breakdown of the idea of ‘a land for Muslims’ since its formation has been in jeopardy. Another interesting part is that while Pakistan was championed as a homeland for Muslims, legally it remains a highly colonial-inspired state in terms of its laws and constitution (Yilmaz, 2016). While it does use Sharia’s guiding principles to form laws, it remains democratic and not purely ‘Islamic’ in its legal and governance aspects (Yilmaz, 2016). This for many hard-line clerics and right-wing groups has added to the identity crises. The exclusive emphasis during its creation on the idea of a ‘land for Muslims’ and the later paradoxes has taken the shape of an ontological crisis for the country. Its foundation of a ‘Muslim land for Muslims’ over the year has been jolted. This existentialist crisis has led to various forms of political and social turmoil in the country for the last seven decades.

Pakistan is a country that has seen violence and brutality since its formation in 1947. Following World War II, the British Raj withdrew from the Indian Subcontinent, creating independent states of India and Pakistan. Pakistan was created as a homeland for the Muslims of the Indian Subcontinent, leading to millions of people migrating across the newly created borders between India and Pakistan. The Great Partition became the largest mass migration event of the twentieth century, but it was also marred by violent hate crimes based on faith, resulting in mass murder, mob lynching, looting, and rape of citizens on both sides of the borders (Talbot, 2009; Menon, 2012; Khan, 2017).

In addition to its traumatic inception, Pakistan has constantly struggled with its identity as a young nation-state. While Pakistan remains a democracy, its track record is tarnished by several military authoritarian regimes. The country has spent decades under four different military dictatorships, one of which took place during 1969-1971, under General Yahya Khan, when Pakistan was facing a civil war in East Pakistan (Sheikh and Ahmed, 2020).
The latest military rule was that of General Pervez Musharraf from 1999 to 2008. While the 2008 general elections have paved the wave for a successive period of democracy the country’s ranking on democratic measures and indexes has remained murky (see Table 1). Various issues such as the lack of freedom of the press, barring the right to protest, arbitrary arrests, enforced disappearances, and gag order on media are a few of the issues apart from poor governance. The military referred to as “the establishment” regularly interferes with democratic processes in the country (Shafqat, 2019). Due to its closeness to the military establishment, Imran Khan’s government during 2018-2022 was called a hybrid regime and similar is the case now under the government-led Pakistan Democratic Movement.

<table>
<thead>
<tr>
<th>TABLE 1 OVERVIEW OF DEMOCRACY IN PAKISTAN</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>The Freedom House (2023)</strong></td>
</tr>
<tr>
<td>Overall score 37/100</td>
</tr>
<tr>
<td>Civil Liberties 22/60</td>
</tr>
<tr>
<td><strong>Democracy Index (2022)</strong></td>
</tr>
<tr>
<td>Overall score 4.13/10</td>
</tr>
<tr>
<td>Electoral process and pluralism 5.67/10</td>
</tr>
<tr>
<td>Functioning of government 5/10</td>
</tr>
<tr>
<td>Political participation 2.78/10</td>
</tr>
<tr>
<td>Political culture 2.5/10</td>
</tr>
<tr>
<td>Civil liberties 4.71/10</td>
</tr>
<tr>
<td><strong>Human Freedom Index (2022)</strong></td>
</tr>
<tr>
<td>Overall rank 146 out of 165 countries</td>
</tr>
<tr>
<td>Personal freedom 5.2/10</td>
</tr>
<tr>
<td>Human freedom 5.44/10</td>
</tr>
<tr>
<td>Economic freedom 6.03/10</td>
</tr>
<tr>
<td><strong>Reporters Without Borders–World Press Freedom Index (2023)</strong></td>
</tr>
<tr>
<td>Rank 150 out of 180 countriesScore is 39.95</td>
</tr>
<tr>
<td>Political indicator rank 139/180</td>
</tr>
<tr>
<td>Economic indicator 136/180</td>
</tr>
<tr>
<td>Legislative indicator 130/180</td>
</tr>
<tr>
<td>Social indicator 140/180</td>
</tr>
<tr>
<td>Security indicator 176/180</td>
</tr>
</tbody>
</table>
In addition to these troubles, the country has been facing waves of home-grown terrorism and mushroom growth in far-right vigilantism from right-wing Islamist groups since the early 2000s. Despite successive military operations and some ‘peace building’ efforts the year 2023 marks the return of radical Islamists (Tehrik-e-Taliban Pakistan and other armed groups) in various areas of the country which results in numerous violent incidents such as conflicts with security forces or targeting civilians by suicide bombing (Jadoon, 2021). Similarly, radical Islamic groups, in both urban and rural areas have spread a culture of vigilantism or ‘mob justice’ where vandalism, physical attacks on people and at times mob lynching have become common practice to show discontent over blasphemous comments by international leaders, local politicians and many times average citizens accused of blasphemy (Yilmaz and Shakil, 2022). In addition, targeting non-Muslims and sectarian minorities in the name of ‘protection of Islam’ these violent mobs has resulted in deaths, vandalism of worship places and loss of property of the victim’s (Yilmaz and Shakil, 2022).

The overview of the country’s current political situation is quite grim. During this chaos surrounding poor governance, a tradition of authoritarianism, military interference, radicalization and disregard of human rights, the country has become a fertile ground for digital authoritarianism as well. Since the late 2000s and through the 2010s the state has replicated its oppressive tactics on the online realm as well.

The last section of this report presents the history and current situation of digital authoritarianism.
DIGITAL AUTHORITARIANISM IN PAKISTAN

The way modern humans interact with information has been fundamentally transformed by the Internet. Nowadays, anyone with a secure connection to the World Wide Web has access to a wealth of information that is freely and readily available. However, this easy access to information has led to an increasing demand for internet governance (Kurbalija, 2016), which refers to the creation and management of rules, policies, and practices in the digital realm. How internet governance is carried out varies from country to country. For example, in India, internet blackouts are commonly employed to suppress protests against the government, thereby violating citizens’ right to protest (Momen and Das, 2021). Yang and Muller’s research on China’s internet censorship demonstrates how authoritarian governments can shape public opinion and quell potential resistance through cyberspace governance. Even in Western democracies, internet governance has sparked significant debates, particularly concerning the state’s surveillance of citizens (Zajko, 2016). Despite concerns about overreaching internet governance, its implementation is justifiable as it helps combat hate speech online, restricts access to child pornography, and flags other potential criminal activities (Kurbalija, 2016). There are also various institutions involved in shaping the internet governance framework, including state institutions, telecommunication companies, international organizations, digital businesses such as social media giants, and civil society.
Pakistan is governed under the 1973 Constitution. Under this legal document, Article 14 of the Constitution of Pakistan guarantees the right to privacy to its citizens (GOP, 2012). The concept of “privacy of the home” in the article is extended and interpreted to digital communications. However, in the article, the freedom or right to privacy is subject to law under various circumstances, which means this freedom is not absolute. In addition, before the advent of the internet, the colonial law Telegraph Act from 1885 and the colonial-inspired Pakistan Telecommunication (Re-organization) Act, of 1996 governed the communication (PTA, 2023). Both Acts under clauses allowed for mass surveillance over the telephone and other forms of communication. Even before 2016, when the first law to govern digital space came into being, the Fair Trial Act, 2013 allows for the mass gathering of surveillance evidence of the accused which has enabled a culture of mass surveillance in the country. The country’s roots in colonial laws, which was itself authoritarian and its continued use of surveillance through successive laws ensured that even without a digital governance bill, their plenty of room for constantly monitoring online activities.

It is also important to understand who uses the internet in Pakistan, so it is clear who are the ones most impacted by a host of new laws and programs designed for the internet governance in Pakistan. In 2005, the internet penetration rate was 6.3 percent but it almost tripled to 15.51 percent in 2017 and was 36.7 percent at the start of 2023 (Kemp, 2023). While this rate might be lower than the global South it is a significant number as over 87.35 million Pakistanis use the internet and, nearly 4.4 million people started using the internet just between 2022 and 2023 (Kemp, 2023). This exponential growth can be explained by not only the increase in the presence of the facility but also by the fact that during the last census, conducted in 2017, nearly 40 percent of Pakistani citizens are under the age of 14 years (UNDP, 2019). This census also indicates a youth dividend in the country saying that “64 percent of the nation is younger than 30 and 29 percent of Pakistanis are between 15 and 29” (UNDP, 2019). This youth bulge can be responsible for an increased appetite for intent consumption. Despite the rapid increase in internet unsafe, it is important to remember that two-thirds of the population does not have access to the internet (Kemp, 2023). Despite this gap, over the last decade, the government has focused its energy on extending its governance to the digital realm.

It is also important to note that Islamist elements enshrined by political parties in power along with the “establishment” (military involved in the politics of the country) also reflect in digital governance. While it is common to use cyber tools to curb freedom of speech of civilian protests and political opposition, it has also become common practice to justify closing websites such as Wikipedia and platforms such as Facebook and YouTube out of respect for “Islamic values and sentiments” (Yilmaz and Saleem, 2022; Yilmaz, 2023). For instance, former Prime Minster Imran Khan has openly advocated for banning content he deems “dangerous” for Muslim youth’s consumption.
He said, “Character building is very crucial in the modern tech-savvy era. The proliferation of tech gadgets and 3G/4G internet technology has made all sorts of content available to everyone […] We need to protect our youth, especially kids, from being exposed to immoral and unethical content available online” (Jamal, 2021). Khan is not alone as various other political parties have a history of banning social media platforms because of accusation of publishing “blasphemous” content. This practice of banning websites or issuing them ultimatums to remove blasphemous content has been set in motion since the first ban of Wikipedia in 2010 (Zaccaro, 2023). At the same time, the establishment has been using its public relations agency, Inter-Services Public Relations Pakistan (ISPR), to let citizens know of the bangers of “foreign” content in online space. They term this a “fifth generation warfare” which is propagated by the alleged “Jewish lobby,” “India” and other “foreign powers” to hurt and misguide Pakistani citizens (Yilmaz and Saleem, 2022). To curb this “fifth generation warfare” the ISPR has mixed jingoism with Islamist jihadist ideals to ensure that the public remains “safe” from these influences on online platforms. In such an eco-system, the state actively targets political opposition leaders, journalists, and human rights defenders, through its vast web of cyber governance which makes the state activities digital authoritarian.

DIGITAL GOVERNANCE

In 2014, the government of Pakistan addressed internet governance by developing a legal framework. This resulted in the creation of the Prevention of Electronic Crimes Act (PECA), which aimed to combat the misuse of electronic media and technology. The Act was passed by the Pakistani parliament in August 2016 and became effective in November of the same year. Pakistan, like many other countries, experienced a significant increase in the use of electronic media and technology. While these developments brought numerous benefits, they also posed challenges such as cybercrime, extremist propaganda, and hate speech on the internet. The PECA was formulated to tackle these challenges and establish a legal structure for addressing cybercrime while safeguarding the rights of citizens in the digital realm.

The Act encompasses a wide range of offences, including hacking, identity theft, cyberstalking, and cyberterrorism. It imposes strict penalties for those found guilty of committing such crimes. It is important to note that at the time, Pakistan was dealing with severe terrorism issues, and the PECA was presented as a vital measure for counterterrorism efforts. This context played a significant role in its swift approval within approximately a year and a half of the draft bill being presented in the National Parliament. However, critics have expressed concerns about the potential for abuse, the impact on freedom of expression, and the privacy implications of the Act. Some argue that it could be used to suppress dissenting voices and restrict access to information (Aziz, 2022). Criticisms also focus on the Act’s vague definitions of offences, lack of oversight, and accountability in its implementation.

PECA includes several key components of internet governance. It grants increased authority to public
institutions such as the Pakistan Telecommunication Authority (PTA) and the Federal Investigation Agency (FIA) for digital surveillance, data collection, and prosecution. The PTA has broad powers under Section 37 of PECA to block and remove content based on ambiguous criteria, often justifying these actions by claiming certain platforms promote “vulgarity” or “corruption of youth.” Additionally, the Act requires social media companies operating in Pakistan to comply with the law and remove any unlawful content within 24 hours of being notified by authorities. Failure to do so can result in significant fines. The government has also mandated these companies to establish local offices in Pakistan and appoint designated representatives to collaborate with law enforcement agencies.

Pakistan has invested resources to strengthen its control over the use of digital technologies in the country. PECA established a comprehensive legal framework for identifying and addressing electronic crimes, including methods for investigation, prosecution, and adjudication. Some articles of the Act specifically focus on terrorism-related online material, including hate speech. While the implementation of PECA is viewed by the state as a crucial step in counterterrorism efforts, its controversial aspects and potential impact on freedom of expression have raised concerns. Nonetheless, the Act received unanimous approval in both the Senate and the National Assembly, as all political stakeholders recognized the significance of counterterrorism measures.

Since 2016, Pakistan has created a host of laws and amendments to govern cyberspace. The foundational law which governs cyberspace is called the Prevention Electronic Crimes Act (PECA). According to Section 21 (d) of this legislation, “Whoever intentionally and publicly exhibits or displays or transmits any information which cultivates, entices or induces a natural person to engage in a sexually explicit act, through an information system to harm a natural person or his reputation, or to take revenge, or to create hatred or to blackmail, shall be punished with imprisonment for a term which may extend to five years or with fine which may extend to five million rupees or with both” (GOP, 2016, 11). While on the surface the law seems a needed measure to curb cybercrime has cyberbullying, hacking and a tool to curb child pornography rings as well as a means to combat terrorism, it is quite ambiguous in its definition of a “cybercrime” which makes it rampart available for abuse in the hands of the oppressive state apparatus (Shad, 2022).

In addition to being vague, the laws grant the Federal Investigation Agency (FIA) unrested powers when it comes to surveillance on social media as well as grant the permission to retain data and seize digital tools (GOP, 2016). This law has paved the way for the state to heavily invest in technology to govern cyberspace. For instance, in 2018 the Pakistan Telecom Authority (PTA) purchase a “web monitoring system” from Sandvine which uses DPI technology (Ali & Jahangir, 2019). Again, the hands of FIA and the military-operated Inter-Services Intelligence (ISI) have been used to carry out mass surveillance of anyone deemed a threat via well-established
social media monitoring cells as a means to counter “threats” and “terrorists” (Pasha, 2017).

In addition to legal measures, the state has redefined the role of the National Database and Registration Authority (NADRA). The agency is a national database, but its role has been expanded. In a shocking revelation in a WikiLeaks document, biometric data of Pakistani citizens from NADRA was provided to Government Communications Headquarters (GCHQ) and National Security Agency (NSA) to investigate “terrorists” (Digital Rights Foundation, 2022). In 2016 and 2018, various ‘safe city projects’ were launched in Islamabad and Lahore, respectively. These projects were part of the China-Pakistan Economic Corridor (CEPC) which ushered in a new wave of collaboration between the two countries. The safe city projects were built on a loan from the Export–Import Bank of China and featured a collaboration between Huawei, National Engineering Services Pakistan (NESPAK) and Arup which installed mass surveillance devices to track criminal activities but also record citizens’ movements via cameras, vehicle number plate tracking, tracing telecommunication communication, drone footage, facial recognition software, etc. (Ahmed, 2021).

Again, while these efforts are showcased as means to curb crime, there has been little proof of this. For instance, in Islamabad, the crime rate rose by 33 percent in 2016, a year after the system was implemented and the country’s national crime rate rose by 11 percent by 2018 (Hillman and McCalpin, 2019). The surveillance system aids the state in mass monitoring citizen activities which often targets political and social opposition from both political and non-political resistance groups.

In addition to laws and technologies to aid cyber governance, the state has showcased a history of blocking internet access to maintain “law and order” since the early 2010s. The PTA has been the manager of this domain where it often restricts internet access at certain times and in specific regions. One of the most frequent justifications for this action is curbing terrorism. For instance, during religious gatherings (e.g., Ashura for the Shi’as) and political demonstrations, internet shutdowns have become a norm in the main law and order (Kamran, 2017). These shutdowns are quite often targeted to remove the spread of information regarding political opposition. While in power, the Pakistan Tehreek-i-Insaf (PTI) used the same mechanism to curb online coverage rallies by its political opposition the Pakistan Muslim League- Nawaz (PLM-N), now out of power, PTI gatherings in Lahore are victim to internet blackouts in the same manner (Raza, 2023).
In addition to gaging websites, internet blackouts are a routine procedure. Historically internet shutdowns were usually put in place to stop terrorist activities on days of religious significance when people gathered in mass such as the processions at Ashura, rallies of Eid Milad-un-Nabi, (Prophet Muhammad’s birthday) or events where people gathered for mass payers such as Eid-ul-Fitr and Eid-ul-Adha. However, these have now expanded to the government using these bans to target the opposition. For instance, in 2021 former Prime Minister Nawaz Sharif was invited to give a talk at an event called Asma Jahangir Conference. Due to a self-imposed exile, Sharif took part in the event via an online address which was blacked out via a targeted internet shutdown since the politician voiced his discontent with the electorate.

**EXAMPLES OF DIGITAL AUTHORITARIANISM**

One of the most prominent examples of digital authoritarianism in Pakistan is showcased via its banning and blocking of content on the internet. As discussed, the most prominent reason for this gaging is the need to protect people from blasphemous or false information. YouTube was banned between 2012-2016 in the country when a video surfaced mocking Prophet Muhammad (Wilkers, 2016). Similarly, TikTok was also banned on two separate occasions, in 2020 and 2021, for "immorality and obscenity in the country" for a few days each time (Masood, 2020). PTA has also banned Twitter several times over the last ten years for various periods in years 2012 and 2021 and all times it was banned because of the spread of sacrilegious content (Verma, 2021; Reuters, 2012).

Photo: Aleksandar Malivuk.
has also been employed to suppress dissent, creating another dimension to the issue. The state’s overwhelming focus on national security, particularly in countering terrorism, has resulted in neglecting its responsibilities under domestic laws, as well as international agreements like the International Covenant on Civil and Political Rights and the Convention against Torture. Despite frequent incidents of data breaches and scandals involving the unauthorized release of audio and video recordings of influential political figures, judges, and journalists, there are no laws in place to safeguard against the collection of personal data and protect privacy. Civil society organizations in Pakistan have expressed concerns regarding the increasing surveillance of both the public and specific individuals such as journalists, politicians, and human rights activists (Pl, 2015). They view these measures as infringements on the right to privacy. Intelligence agencies like the FIA (Federal Investigation Agency) and Inter-Services Intelligence (ISI), along with other authorities overseeing safe city projects, have enhanced their surveillance capabilities by establishing social media monitoring cells (Ahmed, 2021; Azeem, 2019; Yousafzai, 2023). While legal provisions permit digital surveillance for counterterrorism purposes such as blocking hate speech content, it appears that the state is utilizing its expanded surveillance capacity to suppress dissent (Aziz, 2022; Rehman, 2020).

Safe cities employ video cameras and other digital technologies to monitor and identify suspicious activities. Although safe cities encompass various ICT capabilities used in urban establishment and the then-ruling PTI-led government (The News, 2021a). Conversely, in 2023, with PTI out of power, the former opposition formed an alliance government and in May 2023 Imran Khan was arrested for not appearing in several court cases. After this arrest mass protests by PTI supporters sprang across major cities in the provinces of Punjab and KP (Mao, 2023). This led to a blanket internet shutdown to curb protests for over four days (Mao, 2023). In addition, internet blockage is quite a routine matter in Western Pakistan in regions of Swat, FATA, adjoining areas, and parts of Baluchistan where military security forces regularly clash with terrorist groups ranging from separatist groups to jihadist factions (Yilmaz and Saleem, 2022). Internet surveillance has also peaked in Pakistan and the Pakistan military has been the major stakeholder involved in this process. In 2021, a bill was passed ensuring anyone who abused the military could face jail time and hefty fines (Abbasi, 2021). This bill has been instrumental in expanding surveillance on “anti-state” activities and punishing the accused. In May 2023, PTI protesters led to the rioting of public property, which resulted in the rioting of the Prime Minster promising that “all technology available” would be used to punish vandals or some Ministers have been calling them “terrorists” (Sharif, 2023). Similarly, after the unrest calmed down, various videos have surfaced showcasing security forces and agencies using surveillance data to target peaceful protestors as well (Haq, 2022).
areas, the concept of ‘Smart Cities’ goes beyond that of ‘Safe Cities.’ The notion of Smart Cities involves providing internet connectivity and may progress to include electronic payment options for essential services and AI-controlled monitoring devices. Smart cities utilize technologies like high-speed communication networks, sensors, and mobile apps to enhance service delivery, improve mobility and connectivity, stimulate the digital economy, and overall enhance the well-being of citizens (Muggah, 2021; Goulding, 2019). To achieve this, vast amounts of data are leveraged to optimize various city functions, such as utilities, services, traffic management, and pollution control. The rapid expansion of smart city infrastructures globally has sparked controversy due to concerns over the widespread collection, retention, and manipulation of personal data by entities ranging from law enforcement agencies to private enterprises.

In Pakistan, successive administrations have collaborated closely with China to develop secure city infrastructure across urban areas. The Punjab Safe Cities Authority (PSCA), headquartered in Lahore, is a well-known initiative in this regard. With over 6,000 cameras and sensors installed at more than 1,500 locations in Lahore, the Punjab Police, with assistance from the PSCA, can manage traffic, combat crime, and respond to emergencies (Malik, 2022). Notably, Huawei from China has been responsible for constructing all secure city systems in Pakistan. The first safe city system in Islamabad was completed in 2016 through collaboration between the National Database and Registration Authority (NADRA) of Pakistan and Huawei, with funding from China’s EX-IM Bank (Hong, 2022). Another safe city system was established in Lahore in 2018, with Huawei leading the construction and National Engineering Services Pakistan (NESPAK) and UK-based multinational firm Arup providing consultancy and technical support (Ahmed, 2021).

The safe city infrastructure gathers information across several categories, including personal data, vehicle and traffic data, criminal profiles, crime statistics, and parking information. Given the past instances of data breaches within the NADRA database, experts have raised concerns about data security risks. In 2019, several CCTV camera images from Lahore were posted online, featuring inappropriate sexual content (Azeem, 2019). Pakistan’s safe city surveillance systems incorporate facial recognition, artificial intelligence, vehicle number plate tracking, dedicated telecommunication networks, data centers, drones, mobile applications, and intelligent transportation systems.

The effectiveness of Huawei’s safe city infrastructure in reducing urban crime has been subject to debate. Huawei has claimed in a questionable presentation that its safe city solutions significantly reduce crime, increase case clearance rates, shorten emergency response times, and enhance citizen satisfaction. However, investigations by the Center for Strategic and International Studies (CSIS) have indicated that these claims have been greatly exaggerated, if not entirely
are subjected to torture and coerced into making public apologies, with videos of their apologies subsequently released on social media platforms (Dawn, 2022a).

The level of surveillance implemented in Pakistan is linked to an authoritarian approach. Surveillance capabilities are being employed for political purposes rather than solely for the defense of the country or public good. Recorded videos obtained through surveillance serve as leverage for those working behind the scenes, allowing them to exert control by capturing and disseminating compromising material (Khan, 2023; Dawn, 2022b). The timing of the video releases is crucial. Detailed records are maintained on important politicians, indicating a potentially illegal and unconstitutional practice that is incompatible with a democratic society. The impact of these authoritarian measures is evident, as journalists increasingly practice self-censorship and exercise caution in their smartphone usage. Awareness of traceability and concerns over the hacking of email and social media accounts have led to heightened vigilance among social media activists, journalists, and political leaders. However, despite the challenges, Pakistanis continue to find ways to express their opinions, often resorting to satire as a means of circumventing restrictions. Notable media personalities, such as Anwar Maqsood, have managed to avoid trouble by indirectly criticizing state institutions.

Despite the state’s justification that safe city projects primarily serve counterterrorism efforts, it is evident that surveillance technology is being selectively employed. While it is used to counter terrorism and publicly release videos of terrorists involved in major attacks, such as the one in Peshawar in 2023, it is also increasingly utilized to target individuals critical of the government, its officials, and state institutions like the army (Gul, 2022). Examples have emerged of facial recognition technology being used to track down and apprehend individuals who verbally attacked government figures (Nadeem, 2022). Numerous cases have been documented where people have been detained by authorities for posting critical comments on social media. In these instances, individuals

(Hillman and McCalpin, 2019).

In Islamabad, the crime rate continues to grow and there was an increase of 141.2 percent recorded from 2021 to 2022 (Azeem, 2022). Participants in research studies have expressed skepticism, stating that they have not witnessed any positive outcomes or reduction in crime rates because of the safe city projects. A local journalist shared the following views: “For example, in Islamabad, we see that more than 2,200 cameras are installed in only one city. But if we talk about Lahore city there are more than 6,000 cameras installed. They enable the government to monitor the movement of people. They claim that they have installed them to control the law and security situation in cities and to control the crime rate in Pakistan, but we have not seen any positive outcome in that regard through a reduction in the crime rate” (Baloch, 2022).

The judiciary in Pakistan has been a significant source of resistance against the growing digital authoritarianism and digital control
This is mainly because Pakistan is home to a strong network of civil society organizations that also work closely with relevant international organizations to raise awareness on issues relevant, i.e., digital rights. There are several organizations in Pakistan that work for digital rights and strive to protect internet freedom, and privacy, and promote digital literacy. Let us look at some of the prominent organizations in this space in Pakistan. Digital Rights Foundation (DRF) is a non-profit organization that focuses on the advocacy of digital rights in Pakistan. They work on various issues, including online harassment, data protection, freedom of expression, and women's digital rights. DRF conducts research, provides legal assistance, and offers digital security training and awareness programs.

Bolo Bhi is a civil society organization that advocates for open access to information, digital security, and internet freedom in Pakistan. They engage in policy advocacy, conduct research, and provide digital literacy training. Bolo Bhi also works to raise awareness about online censorship, surveillance, and privacy issues.

Media Matters for Democracy (MMfD) is a non-profit organization that focuses on media development, digital rights, and freedom of expression in Pakistan. They work towards promoting online civic spaces, digital literacy, and defending digital rights through research, policy advocacy, and capacity-building programs.

Internet Policy Observatory Pakistan (iPOP) is a research-based initiative that aims to monitor and analyze internet governance measures implemented by the state. This ongoing process involves various legal cases under the PECA, the authority of institutions like the Federal Investigation Agency (FIA), and concerns related to data protection and privacy. The PECA Amendment of 2022, which primarily aims to criminalize defamation and make it a non-bailable offence, has faced critical scrutiny from local courts. Human Rights Watch has pointed out that expanding PECA's already extensive provisions on criminal defamation to online statements about government institutions violates Pakistan's international obligations. Media organizations in Pakistan challenged the PECA Amendment in the Islamabad High Court, where Justice Athar Minallah declared the new legal provisions a violation of freedom of speech as guaranteed by Article 19 of the Constitution of Pakistan (Naseer, 2022). The court also instructed the interior ministry to investigate the conduct of the FIA's Cyber Crime Wing due to concerns of power abuse and infringement of individuals' fundamental rights. Justice Minallah emphasized that no one should fear criticism, particularly in relation to defamation and concerns raised by public officeholders regarding social media attacks. As a result, the FIA closed nearly 7,000 cases, primarily related to defamation.

CIVIL SOCIETY ACTIVISM FOR DIGITAL RIGHTS IN PAKISTAN

In many ways, there are still not enough laws in Pakistan to deal with digital rights, but the pressure is growing on policymakers to pay attention to the issues of privacy and data protection.
issues in Pakistan. They conduct policy research, produce reports, and provide recommendations on topics such as data protection, surveillance, and censorship. iPOP also engages in advocacy efforts to promote a free and open internet.

Although not based in Pakistan, Privacy International is a global organization that advocates for privacy rights and challenges surveillance practices worldwide. They work with local partners and provide support in the context of Pakistan to raise awareness, carry out research, and advocate for stronger privacy protections. These organizations actively engage with policymakers, raise public awareness, and work towards protecting digital rights in Pakistan through research, advocacy, and capacity-building activities.
INTERNET ACCESS

With the proliferation of the internet worldwide, several civil society organizations have dedicated their efforts to shed light on the significant issue of inadequate internet access within Pakistan. These organizations aim to amplify the voice of society, urging the government to invest in improving internet access. In this vein, Bytes for All, Pakistan (B4A), is a well-known digital rights organization, that seeks to secure digital rights and freedom of expression for civil liberties. In the end, they organize seminars, workshop training and produce various publications. For example, B4A has published annual reports on internet access in Pakistan (Haque, 2023). The 2022 report shows that there has been some progress in terms of internet access in Pakistan, but the country is still behind many Asian countries. One key finding of the report reveals that despite increased internet penetration, around 15 percent of the population remains without any access, while others face challenges such as slow speeds and inconsistent service, hindering meaningful internet access (Haque, 2023: 5). Pakistan ranks 118th in mobile broadband and 150th in fixed broadband, as per the B4A report (Haque, 2023: 9). The organization also raises concerns about the government’s attempts to restrict the internet and control cyberspace, including filing cases against journalists, activists, and political opponents for expressing unfavorable views on social media and proposing stricter defamation laws to counter dissent. To enhance internet access in Pakistan,
B4A provides several important recommendations. These include recognizing fixed broadband as critical infrastructure and developing a national broadband strategy with a fiber plan. Additionally, improving the investment climate and financing options within the digital ecosystem and streamlining government administration are identified as essential actions for expediting implementation.

Media Matters for Democracy (MMfD) is another Pakistani organization focused on media literacy, digital democracy, progressive media, and internet regulation. They also work on integrating digital media and journalism technologies and creating sustainable initiatives in the media-tech sector. They provide several online free courses in different subjects. For example, their course “understanding citizen journalism” includes 54 lessons and “Digital Disinformation and Journalistic Responsibilities” encompasses 82 lessons (Arsalan, 2023; Khan, Mindeel and Shaukat, 2023). Also, this organization publish research investigations and policy papers. In one of their comprehensive reports, titled “Connecting the disconnected: mapping in digital access in Pakistan,” MMfD highlights that approximately 52.79 percent of Pakistan’s population, equivalent to 116 million people, has access to some form of internet (Kamra et al., 2022: 7). However, the report suggests that despite high tele density indicating cellular service connectivity for nearly 88 percent of the population, there remains a significant gap in internet access, particularly in mobile and broadband services across most parts of the country (Kamra et al., 2022: 16). Accordingly, the number of broadband subscribers stands at 116 million, 3G/4G mobile internet subscriptions at 113 million, and basic telephon subscribers at 2 million, representing only 1.14 percent of the total population (Kamra et al., 2022: 17). This reveals that over 47 percent of the population remains disconnected from the internet (Kamra et al., 2022: 25).

The report stresses that various factors contribute to this gap, with disparities evident between urban and rural areas. The available data does not offer a breakdown based on rural/urban or gender demographics, which are significant barriers to internet connectivity. They also argue that the COVID-19 lockdown further exacerbated these disparities, with individuals in peripheral and rural areas facing challenges due to limited infrastructure, while low-income communities struggled to afford smartphones and internet connections. The organization advocates for ensuring that human and social justice values drive technical development and use in Pakistan by providing some key recommendations. They emphasize the need for policies and regulations related to internet access to follow a rights-respecting model. Also, it is underlined that a core focus should be bridging the digital divide across class, gender, age, and geography as well as increasing digital literacy. In addition, they urge the government to make the Internet economy inclusive, address the need for online social norms, and empower individuals
to shape their futures. Finally, the report emphasizes that building robust, secure, and resilient networks is crucial (Kamra et al., 2022).

Moreover, the efforts of civil society organizations to advocate for internet access are evident in various initiatives. One significant area of concern raised by these organizations is the Citizens Protection (Against Online Harm) Rules, issued in 2020. In terms of the obstacles of this law to internet access, a report published by DRF argued that these rules violate fundamental and constitutional rights, particularly Articles 14 and 19. The analysis emphasizes that these regulations impede the free movement of data, creating artificial barriers to information sharing and hindering global communication. Additionally, they exacerbate the lack of accessibility and affordability of internet connectivity for individuals and businesses. This issue is particularly detrimental as reducing connectivity costs is vital for expanding economic opportunities, promoting the digital economy, and generating wealth in Pakistan (DRF, 2020b).

Bolo Bhi, another digital rights organization, has also expressed concerns about the Citizen Protection laws, highlighting their attempt to gain jurisdiction over social networking platforms and access data. Their objective extends beyond content restriction to encompass accessing communication content and filtering technology. Bolo Bhi points out aspirations to establish local offices and data servers for unrestricted data access, which has been a recurring theme in previous attempts (Bolo Bhi, 2020).

The Human Rights Commission of Pakistan (HRCP), the country’s leading independent human rights body, advocates for internet access and freedom of expression as fundamental human rights in their reports. In a collaborative study titled ‘Freedom of Peaceful Assembly in Pakistan: A Legislative Review,’ released in partnership with the International Federation for Human Rights (FIDH) in March 2022, the HRCP called for a reassessment of the existing legislative framework, which still reflects policing strategies from the colonial era. Regarding internet access, the report proposes granting unrestricted media and digital access during assemblies, promoting freedom of speech and movement, rather than imposing content-based restrictions or blocking routes (HRCP, 2020).

It should also be noted that addressing the significant digital divide in Pakistani society is one of the key challenges in internet access. While limited access to technology is commonly associated with the digital divide, factors such as poverty, illiteracy, lack of computer literacy, and language barriers contribute to this issue in Pakistan. In response, the Internet Policy Observatory Pakistan (iPOP) takes concrete actions beyond workshops and reports. According to their website, they provide computers, communication equipment, software, and training to tackle the digital divide. The organization reports that most low-income households in the country find themselves on the disadvantaged side of the digital and knowledge divide. Consequently, their ability to participate effectively...
in the knowledge society remains significantly underdeveloped and underutilized. This situation puts these households at risk of further marginalization in a knowledge-driven society, where access to and utilization of information technology are just a fraction of the broader challenges they face (IPOP, 2023).

By and large, civil society organizations play a crucial role in advocating for improved internet access and reducing the digital divide in Pakistan. These organizations act as catalysts for change by advocating for policies and initiatives that promote equitable access to technology and bridge the gap between different segments of society. As discussed above, civil society organizations raise awareness about the importance of internet access as a fundamental right and a driver of socio-economic development. They highlight the disparities in access and the barriers faced by marginalized communities, such as low-income households, women, and rural populations. By bringing these issues to the forefront, civil society organizations can create a sense of urgency among policymakers and stakeholders to address the digital divide and make internet access more inclusive.

Moreover, civil society organizations actively engage in research, advocacy, and capacity-building activities to promote digital literacy and skills development. They organize workshops, training programs, and awareness campaigns to empower individuals with the necessary knowledge and tools to navigate the digital landscape. By enhancing digital literacy, these organizations enable individuals to fully participate in the digital age, access online opportunities, and leverage technology for personal and professional growth.

Eventually, civil society organizations play a critical role in monitoring and influencing policy development and implementation. They provide expert analysis, recommendations, and feedback on laws, regulations, and initiatives related to internet access and digital rights. Through their engagement with government agencies, regulatory bodies, and other stakeholders, these organizations attempt to ensure that policies are inclusive, rights-based, and responsive to the needs of diverse communities.

**PRIVACY**

Privacy is an essential aspect of individuals’ rights, encompassing their ability to maintain control over personal information, safeguard it from unauthorized access, and prevent unwanted intrusions. In Pakistan, the right to privacy is constitutionally protected under Article 14, which upholds individuals’ dignity and personal autonomy. However, despite this recognition, several challenges hinder people in Pakistan from effectively protecting their privacy, particularly in cyberspace.

One key challenge is the limited digital literacy among most of the population. In response, civil society organizations play a crucial role in educating the public through campaigns, seminars, research publications, policy reports, workshops, and awareness programs. For example, DRF has published a report,
titled “Young People and Privacy in Online Space”, which aims to raise concern about the privacy of youth in cyberspace (DRF, 2021b). The report acknowledges that despite the ongoing increase in the number of young people users on the internet, and particularly social media, they face insufficient protection and have limited awareness of their privacy rights. The organization suggests that young generations recognize the gendered nature of online harm, particularly impacting women. Therefore, the report emphasizes that it is crucial to foster collaboration to enhance legal frameworks and establish effective mechanisms to safeguard young people’s rights. DRF has also published privacy-related reports that provide up-to-date information regarding digital privacy. They include ‘How to keep your social media secure and anonymous,’ ‘Understand cyber-harassment,’ ‘What to do when there is a privacy breach?’, ‘Protect against viruses and malware’ and ‘Two-factor authentication’ (DRF, 2020a).

Another privacy concern in Pakistan stems from the government surveillance system, which has advanced in recent years. In this vein, civil society organizations and activists in Pakistan have been advocating for stronger digital privacy protections. They have called for greater transparency in government surveillance activities, improvements in data protection practices, and the need for comprehensive privacy legislation aligned with international standards. In 2019, Bolo Bhi raised concerns about the Web Monitoring System (WMS) deployed by the Pakistan Telecommunications Authority (PTA). The WMS aims to monitor and control internet traffic for commercial and security purposes. However, the organization underlined that the lack of safeguards and judicial oversight raises concerns about the potential misuse of surveillance capabilities (BoloBhi, 2019). Bolo Bhi urged the government to take concrete steps to demonstrate the veracity and reliability of its claims that the WMS will not restrict internet freedom. Moreover, the director of this civil society organization suggested that transparency regarding the technology provider, Sandvine Inc, and its security audit is crucial. Public accountability and corporate responsibility should be upheld to align with international principles of human rights, freedom of expression, and privacy (BoloBhi 2019).

Digital Rights Monitor, a project under MMfD, has attempted to contribute to improving digital privacy in Pakistan. They have produced a series of videos, titled ‘Privacy-in-Law: Legal Framework of Digital Privacy Laws in Pakistan’ (Kamran, 2019). These videos provide information about the enacted laws that protect citizens’ privacy and assess their implementation in Pakistan. The videos cover important legislation such as the ‘NADRA Ordinance, 2000,’ ‘The Investigation for Fair Trial Act, 2013,’ ‘The Pakistan Telecommunication (Re-Organization) Act, 1996,’ and the ‘Prevention of Electronic Crimes Act 2016 (PECA).’ They seek to uncover the details of the laws that are aimed at framing data security regulations, regulating law enforcement and intelligence agencies’ power to investigate criminal cases, and...
countering increasing crime originating from cyberspace.

Bytes for All (B4A) has also been active in highlighting the importance of privacy in the virtual world. In 2020, the organization published a report titled, 'The Scope of Privacy Commission in Pakistan,' which strongly advocated for the establishment of an independent and autonomous Privacy Commission free from political or executive influence (Raza and Baloch, 2020). This commission is deemed essential for protecting citizens’ digital data and providing redressal for privacy-related violations. B4A has also conducted personal training sessions on digital privacy and raised public awareness by addressing topics such as the 'Dangers of Digital Surveillance' (Raza and Baloch, 2020). To enhance online privacy in Pakistan, digital rights advocates in this organization, have put forth several recommendations for the government to consider. These recommendations can be summarized as follows (Baloch and Qammar, 2020):

– Revise laws to limit intelligence agencies’ powers in intercepting digital communications and private data of journalists and human rights defenders.
– Define clear criteria for digital surveillance in the context of national security and counterterrorism.
– Cease mass digital surveillance on citizens.
– Promote encrypted communications for the safety of vulnerable groups.

– Include secure communications training in public sector education, especially in journalism and law.

– Respect citizens’ right to privacy, especially journalists and human rights defenders, to strengthen democracy, freedom of speech, and information access.

Civil society organizations actively participate in policy discussions and provide valuable input during the development of privacy-related laws and regulations. They bring the perspectives and concerns of the public to the attention of policymakers, advocating for privacy-focused policies that strike a balance between security and individual rights. Their involvement aims to assess to what extent the government measures align with the principles of transparency, accountability, and respect for privacy. In Pakistan, with the new wave of internet penetration, particularly among young generations, the effort of civil society organizations is essential for fostering a privacy-conscious society and holding governments accountable for protecting individuals’ digital privacy rights. Through their persistent advocacy, these organizations can contribute to a more informed and balanced policy-making process. They provide expertise and recommendations based on research and analysis, offering practical solutions that protect privacy rights while addressing security challenges. Their efforts underscore the importance of privacy as a fundamental right, even in the face of increasing surveillance measures.
aspects of personal autonomy and limiting unwarranted intrusion.

Currently, Pakistan lacks comprehensive legislation specifically governing the processing of personal data. However, like the privacy domain, the Prevention of Electronic Crimes Act, 2016 (PECA) serves as a legal framework to address electronic crimes and unauthorized access to personal data. Under PECA, the Ministry of Information Technology and Telecommunications (MOITT) has established the Removal and Blocking of Unlawful Online Content Rules 2021, granting the Pakistan Telecommunication Authority (PTA) the authority to remove or block access to information systems (Rehman, 2022). The Personal Data Protection Bill 2021, which is awaiting enactment, will become aspects of personal autonomy and limiting unwarranted intrusion.

DATA PROTECTION

Data protection entails safeguarding personal information against unauthorized access, use, or disclosure. It encompasses obtaining consent, employing data for specific purposes, minimizing data collection, ensuring accuracy, implementing security measures, respecting individual rights, and safeguarding data during transfers. Upholding privacy and cultivating trust with individuals is both a legal and ethical obligation. While data protection and privacy are closely related, they carry distinct meanings. Data protection focuses on safeguarding personal information, whereas privacy centers on maintaining control over one’s personal life and information. Data protection ensures the secure handling of data, while privacy encompasses broader aspects of personal autonomy and limiting unwarranted intrusion.

Currently, Pakistan lacks comprehensive legislation specifically governing the processing of personal data. However, like the privacy domain, the Prevention of Electronic Crimes Act, 2016 (PECA) serves as a legal framework to address electronic crimes and unauthorized access to personal data. Under PECA, the Ministry of Information Technology and Telecommunications (MOITT) has established the Removal and Blocking of Unlawful Online Content Rules 2021, granting the Pakistan Telecommunication Authority (PTA) the authority to remove or block access to information systems (Rehman, 2022). The Personal Data Protection Bill 2021, which is awaiting enactment, will become aspects of personal autonomy and limiting unwarranted intrusion.
the primary legislation regulating the processing of personal data in Pakistan. It will apply to individuals and entities that control, process, or authorize the processing of personal data within the country.

Digital rights organizations have actively campaigned for data protection in Pakistan. The Digital Rights Foundation (DRF), for instance, has been proactive in providing feedback on the Personal Data Protection Bill (PDPB). They have submitted various reports to the government to enhance the bill to align with international standards. The organization, Digital Rights Foundation (DRF), has identified several persistent issues in the bill since 2018 that must be addressed to align with global data protection standards and privacy rights. According to DRF, concerns have been raised regarding the broad powers granted to the Federal Government, which could lead to self-interested interpretation and evasion of regulation. They have also expressed concerns about the lack of independence of the National Commission for Personal Data Protection (NCPDP), as it remains under the administrative control of the Federal Government, compromising its autonomy and failing to meet international standards (DRF, 2021a).

DRF has stressed that the requirement for ‘critical personal data’ to be processed within Pakistani servers is impractical and akin to data localization, which could hinder business operations and investment. Ambiguities exist in terms like ‘national interest’ and ‘national security’ without clear definitions, granting the government wide discretion in implementing the law. DRF highlights that the bill also lacks provisions addressing emerging technologies such as automated decision-making and artificial intelligence, necessitating further elaboration and the inclusion of non-discrimination safeguards. DRF emphasizes the need for specific language, defined terms, and adequate safeguards to ensure that the law aligns with legislative intent and effectively protects digital rights.

In addition, B4A Pakistan has published at least 13 comprehensive reports on data protection in Pakistan. These reports encompass various aspects, including submissions to the government for consultation and the creation of training materials. One of their reports, titled ‘Electronic Data Protection in Pakistan,’ provides a thorough analysis of the country’s data protection status and offers key recommendations (Gilani et al., 2017). B4A highlights the concerning absence of data protection legislation in Pakistan, particularly given the increasing volume of citizens’ data being processed daily. Urgent action is required to establish clear and effective data protection laws that meet the demands of the digital era. Failure to do so may lead foreign companies to perceive Pakistan as an unsafe business environment, deterring them from outsourcing their services to the country. B4A provides several recommendations to address these concerns, including (Gilani et al., 2017):

- Amendment to PTA is necessary.

The Protection of Privacy Act
(PTA) of Pakistan is incompatible with Article 17 of the ICCPR.

- There is an urgent need for an independent authority to oversee data protection compliance.

- A system of accountability for data breaches should be established.

- The Authority set up under the draft Bill lacks independence and autonomy.

- The exemptions to the prohibition of processing of ‘personal data’ including ‘sensitive personal data’ are too broad.

- The Bill does not cover intelligence agencies’ collection, storage, and use of data.

Overall, despite Pakistan’s increasing participation in the digital sphere, the government must move quickly to prioritize data protection due to the country’s rapidly expanding online population. In fact, as Bolo Bhi urged, Pakistan should take note of what other developed nations have to say. The government can take the required actions to strengthen data protection safeguards and ensure the privacy and security of its citizens’ personal information by taking note of successful practices already in place abroad. By enacting effective policies and regulations that adhere to international standards, Pakistan must give priority to the rights and well-being of its citizens in the digital sphere.

As a final point regarding the role of civil society organizations in Pakistan in promoting digital rights, internet access, privacy, and data protection, it should be emphasized that they tirelessly raise awareness about these important issues, attempt to facilitate fruitful dialogue between citizens and policymakers, and actively work towards holding those responsible accountable. Through their diligent work, they hope to
greatly contribute to the creation of efficient laws and procedures that uphold the rights of people and promote a safe and welcoming online environment for everyone. To influence decision-makers to meet the requirements of the populace, these organizations offer insightful research-based studies, policy suggestions, workshops, seminars, online and offline training sessions, and periodical audits of internet legislation and privacy rules. Or to put it another way, they try to help.

CONCLUSION

Pakistan’s historical trajectory has been marked by a series of challenges, including violence, religious divisions, and an ongoing struggle to define its national identity. These factors have significantly shaped the current political landscape of the country. Despite its aspirations to establish a stable democracy, Pakistan has faced recurring periods of military rule, which have undermined democratic processes and institutions.

The governance challenges in Pakistan include limitations on press freedom, restrictions on the right to protest, and interference from the military establishment. These issues have raised concerns about the strength and integrity of Pakistan’s democratic system. Furthermore, the military’s influence has often overshadowed civilian governance, leading to complex power dynamics within the country.

In recent years, Pakistan has witnessed the emergence of digital authoritarianism as a governing strategy. This involves using digital technologies and surveillance mechanisms to control and monitor online activities. The government has implemented legislation like the Prevention of Electronic Crimes Act (PECA) to regulate cyberspace. However, the vague definitions of cybercrime within PECA and the broad surveillance powers granted to agencies such as the FIA and ISI raise apprehensions about potential abuses of power.

To enforce digital authoritarianism, the state has invested in advanced technological capabilities for monitoring online communications. This includes the acquisition of web monitoring systems and the establishment of social media monitoring cells. These measures aim to consolidate the state’s control over cyberspace and curtail citizens’ digital privacy.

Nevertheless, Pakistan’s democratic fabric is not entirely eroded. In addition to push back from the judiciary, Pakistan has a strong civil society and there are various human rights organizations, including the ones that exclusively focus on digital rights. Human rights organizations, including those specifically focused on digital rights, play a crucial role in advocating for the protection of digital freedoms in Pakistan. These organizations voice concerns about the need for stronger legislation on data protection and privacy and advocate for equitable access to the internet, especially for marginalized communities in remote regions like ex-FATA and Balochistan.

By highlighting these concerns and advocating for digital rights, civil society organizations and the judiciary serve as important
checks and balances against the encroachment of digital authoritarianism. Their efforts contribute to promoting transparency, accountability, and respect for individual rights in the digital sphere, despite the challenges posed by the current political landscape in Pakistan.
REFERENCES


DRF. (2021b). Young people and privacy in online space. Lahore: Digital Rights Foundation.


Nadeem, Hussain. (2022). “Personal communication, 19 September 2022.”


https://twitter.com/CMShehbaz/status/16573322227671137


https://hdr.undp.org/content/unleashing-potential-young-pakistan


https://doi.org/10.55271/pp0016

https://doi.org/10.55271/pp0001

