DigitalRightsFoundation
"KNOW YOUR RIGHTS"

VOTER DATA PRIVACY IN PAKISTAN

Privacy Risks, Data Protection, and Legislative Shortcomings during Data-Driven Elections

ABOUT DIGITAL RIGHTS FOUNDATION

January 2025

Researched and co-authored by: *Maryam Ali Khan, Ashus Owaisi, and Zainab Durrani.*
Edited by: *Adnan Chaudhri, Seerat Khan, Talal Raza, and Maryam Ali Khan.*
Design and Layout by: *Ahsan Zahid and Talha Umar.*

Digital Rights Foundation (DRF) is a women-led, not-for-profit organisation based in Pakistan working on digital rights freedoms since 2013. DRF envisions a place where all people, especially women and gender minorities, can exercise the right of expression without being threatened. DRF believes that a free internet with access to information and impeccable privacy policies can create safe online spaces for not only women but the world at large.

At DRF, we aim to strengthen the protections for human rights defenders (HRDs), with a focus on women's rights in digital spaces through policy advocacy and digital security awareness-raising. In addition, one of our main aims is to protect women from cyber harassment that they have to deal with throughout their lives by making them aware of their rights and making resources accessible when they need help.

With growing privacy concerns in digital spaces, DRF seeks to increase awareness about privacy issues and defend the right to privacy through research, monitoring and reporting the tactics around surveillance. To rally with other actors for strong legal protection for privacy in the country and to raise our voices against dictating censorship policies, we propose viable solutions to the government and other authoritative bodies.

Contact information:
info@digitalrightsfoundation.pk
www.digitalrightsfoundation.pk

ACKNOWLEDGMENTS

This report is an important part of the discourse DRF hopes to foster around data privacy and voter rights in Pakistan. This project would not have been possible without the efforts of the DRF team and the invaluable contributions of participants who generously took the time to share their insights and experiences. We hope that this report honours their narratives.

DRF would also like to acknowledge the support and direction provided by Privacy International (PI) in shaping the report.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Pakistan's 2024 General Elections, held in February, witnessed an increased use of technology and social media tools, echoing the role and pace of digital transformation during, and in the run-up to, electoral events across the globe. Though the increased integration of technology in electoral processes has shaken up how data is navigated and interpreted across the world, bringing with it potentially significant benefits, it has also introduced critical challenges related to data privacy and voter surveillance.

The aim of this study is to explore these challenges, especially in the context of Pakistan's 2024 elections, which brought renewed scrutiny to the issue of voter data privacy, particularly in the light of recent reported cases of data breaches at the country's national citizen database authority - the National Database and Registration Authority (NADRA) - as well concerning reports of data misuse during recent political party campaigns. Concerns were raised by voters and observers regarding a recent trend wherein voters reported receiving automated calls from candidates and political party representatives, in the run up to the elections. This in turn raised a pressing question: Where did these parties obtain voters' personal data, including their contact information? This strikes at the heart of broader concerns about who holds and controls citizens' data in Pakistan. This research report explores these issues, analysing the mechanisms through which voter data is handled, and potentially misused during the electoral process, with a focus on the implications of the 2024 elections.

The report also aims to deduce the roles that the Election Commission of Pakistan (ECP) and NADRA played regarding the handling of voter data during the 2024 elections in Pakistan, and analyse how personal data, which covers names, CNIC numbers, addresses, contact numbers, and voting numbers et al are made accessible, which allows third parties to potentially leverage said data for voter surveillance.

To gauge a better understanding of voter data misuse, we conducted a nationwide survey of 271 people. We also interviewed a total of 6 voters: two from Punjab, one from Khyber Pakhtunkhwa, one from Sindh, one from Balochistan and one from the federal capital, Islamabad. Additionally, the researchers also interviewed candidates from 5 political parties who contested the elections in February 2024. This includes Pakistan Tehreek-e-Insaaf (PTI), Haqooq-e-Khalq Party (HKP), Pakistan People's Party (PPP), Awami Workers Party (AWP) and Jamaat-e-Islami (JI). According to the data we collected, some calls were automated and played pre-recorded messages by prominent party leaders, such as Imran Khan (PTI), and Shahbaz and Nawaz Sharif (Pakistan Muslim League (N)), requesting support for their respective parties. Targeted calls were also made by political party representatives requesting support for candidates running in voter-specific constituencies. Though this strategy may be an effective way to capture voter attention, it raises significant concerns about the state of voter data privacy in Pakistan, particularly given that Pakistani citizens have no legal protection for their data. Despite numerous

drafts of the proposed Personal Data Protection Bill spearheaded by the Ministry of IT and Telecom (MoITT) since 2018, Pakistan has yet to enact a data protection law leaving Pakistani citizens vulnerable to unchecked data privacy violations.

It was clear through our research that the digitisation of politics in Pakistan raises significant concerns regarding privacy and democratic integrity - especially given the aforementioned lack of data protection legislation in Pakistan. That absence allows political parties and other third parties to access and misuse personal citizen data for micro-targeted messaging, sometimes without ever taking any form of prior consent, without apparently any penalties for doing so. This modus operandi, coupled with weak regulatory frameworks, leaves Pakistani citizens vulnerable to exploitation, and runs the risk of weakening what faith they may have in government institutions, including the parties they may support. It is vital that data privacy frameworks are strengthened, with the implementation of rigorous auditing systems for data authorities, telecommunication companies, and government institutions being essential measures required to safeguard the data privacy of voters, and to restore or reaffirm trust in the electoral process.

INTRODUCTION

The increasing integration of technology into elections has revolutionised how voter[1] data is collected, managed, and utilised in many countries around the world. This digital transformation has brought about significant benefits, such as more efficient voter registration and targeted campaigning. However, it has also introduced critical challenges related to data privacy and voter surveillance.

The 2024 general elections in Pakistan, held on 8th February, brought renewed scrutiny to the issue of voter data privacy, especially with the increasing use of technology in political campaigns. Concerns were raised over a new trend where voters received calls from candidates and political party representatives, colloquially referred to as 'robocalls', in the weeks preceding the elections. According to some of our interviewees, some calls were automated and played pre-recorded messages by prominent party leaders, such as Imran Khan and Shahbaz and Nawaz Sharif, requesting support for their respective parties (Durrani, 2024). Targeted calls were also made by political party representatives requesting support for candidates running in voter-specific constituencies. While this strategy may be an effective way to capture voter attention, it raises significant concerns about voter data privacy in Pakistan which has 193 million mobile cellular subscribers with a tele-density of 79.413%, as reported by the Pakistan Telecommunication

1 Throughout this study, "voter" will be used to refer to individuals who were registered to vote and whose personal data was collected and used by political parties as a part of their election campaigns, regardless of whether they voted or not.

Authority (PTA).[2] To exacerbate matters, Pakistani citizens have no legal protection for their data. Despite numerous drafts of the proposed Personal Data Protection Bill spearheaded by the Ministry of IT and Telecom (MoITT) since 2018, Pakistan has yet to enact a data protection law leaving Pakistani citizens vulnerable to unchecked data privacy violations.

This lack of regulatory protection exacerbates the existing mistrust in the system, particularly when individuals receive unsolicited communication from political parties vying for electoral seats. The immediate and pressing question for many is: Where did these parties obtain their contact information? This question strikes at the heart of broader concerns about who holds and controls citizens' data in Pakistan. This research report seeks to explore these issues, analysing the mechanisms through which voter data is collected, shared, and potentially misused during the electoral process, with a focus on the implications of the 2024 elections (Durrani, 2024). In particular, it aims to deduce the role the Election Commission of Pakistan (ECP) and the National Database and Registration Authority (NADRA) played in handling voter data during the 2024 general elections in Pakistan and analyse how personal data, which covers names, CNIC numbers, addresses, contact numbers, and voting numbers, is made accessible, allowing third parties[3] to potentially leverage it for voter surveillance. This allows us to shed light on the existing vulnerabilities in Pakistan's current data protection mechanisms and electoral processes, by further analysing the gaps in Pakistan's existing legal framework, including the Election Act 2017, as well as more recent developments like the Personal Data Protection Bill 2023.

Furthermore, the study explores voters' perceptions and understanding regarding the unauthorised use of their personal data, as well as their knowledge of existing legal frameworks that could potentially protect them. This offers more insight on whether these laws adequately protect the data rights of citizens, particularly during sensitive national events like elections, when there are high chances of data misuse (Privacy International, 2019). By comparing Pakistan's situation with other countries in South Asia, such as India, where the Aadhaar card system plays a similar role, Malaysia, and Sri Lanka our analysis will offer a broader regional perspective on the challenges and opportunities in protecting voter data. Ultimately, this research intends to contribute to the ongoing discourse on data privacy in Pakistan, emphasising the need for robust data protection laws and more transparent practices by electoral bodies and political entities. By addressing these issues, the study aims to inform key stakeholders—including the government, judiciary, and civil society, as well as political parties, NADRA, and ECP — about the critical importance of safeguarding voter data to uphold the integrity of elections and maintain public trust in the democratic process.

2 These statistics were last updated in August 2024, at the time of the writing of this report.

3 In this context, third parties refer to entities such as political parties, telecommunications companies (as noted by a voter interviewee on page 28), educational institutions, and brands that purchase citizen data for marketing purposes.

METHODOLOGY

The methodology employed for this report is a mixed-method approach consisting of survey forms and qualitative interviews to understand and map the impact of the 2024 electoral cycle on privacy rights of voters in Pakistan.

The exception to the geographical setting of Pakistan chosen for this research was that of Gilgit Baltistan and Azad Jammu and Kashmir, as these two regions while within the borders operate on a different electoral cycle and did not participate in the 2024 general elections. The report looks towards political parties, NADRA and the ECP as the key stakeholders.

The first round of data was collected through a survey, designed to gather information regarding perceptions, and methods of voter data misuse. This survey was available in English and Urdu - a decision made on the basis of previous data collection experience and an interest in casting a wider net amongst the population. A total of 271 responses were collected with 138 of the responses received coming in from the English survey form and 133 from the Urdu version.

The second round of data collection was done through qualitative interviews held virtually. Two stakeholder sets were engaged at this stage, voters and political parties.

For the first set, the researchers interviewed a total of 6 voters: two from Punjab, one from Khyber Pakhtunkhwa, one from Sindh, one from Balochistan and one from the federal capital, Islamabad. The interview questions set to the voters spoke to their impression of any usage of their personal data without consent as well as their feedback on data protection.

For the second set, the researchers engaged with 5 political parties whose candidates contested the elections in February 2024. This includes PTI, HKP, PPP, AWP and JI. Despite months of reaching out to multiple candidates within the party, no member of the ruling Pakistan Muslim League (N) (PML-N) agreed to speak on record about voter data privacy. The interview questions were set to inquire the impact of social media campaigning during elections, the policies and methods employed by political parties during election campaigns as well in terms of processing and storage of voters' data and their opinion on transparency on the subject of political advertisements.

A third, independent interview was also conducted with the ex-Chairman of NADRA, whom we will refer to as X throughout this report in order to respect anonymity. This interview helps us in visualising the structure of content on the national database within this report, as well as forming a separate section covered within the main body.

All 3 sets of interviews were conducted virtually, given the geographical spread of the participants across the country and the fact that the DRF research team is based in Lahore, Pakistan. So, in the interests of capacity and flexibility, the decision was made to conduct these interviews online.

LIMITATIONS

The study's limitations included limited geographic reach, time, access, and stakeholder/interview subjects' availability. As the research team is primarily based in Lahore, Punjab, the networks developed and created and the stakeholders that could be accessed are primarily in the Punjab province, thus a significant portion of the data collected was Punjab-centric and lacked a balanced regional diversity, though was not completely devoid of it.

Owing to the team being based out of Lahore, it was difficult to carry out in person interviews due to limitations on time and resources. To maintain consistency, all interviews, even for participants based in Lahore, were conducted via Zoom.

The second limitation was the lack of time in terms of data collection to include more voter and political party interviews, given the schedule of an average policymaker/politician there was a larger time lag between requesting an interview and the agreement to sit down for one, thus increasing the time cycle for the data collection. This time constraint was particularly evident when the team was attempting to reach out to members of the ruling party, PML-N. Despite reaching out to five party candidates over the span of five months, we ran out of time to acquire their perspective on the issue, which would have been highly valuable for our discussion.

Thirdly, the political climate in the country put the researchers at a disadvantageous position as reaching out to intended stakeholders became a much harder task than anticipated given the political developments and situation they were embroiled in.

BIG DATA, BIG RISKS: BIG DATA EXPLOITATION IN ELECTIONS

"Big data" refers to large datasets that typical database software would be unable to effectively capture, store, manage, or analyse. This definition has been intentionally left flexible, as what qualifies as big data evolves with technological advancements. The threshold for big data can change depending on the industry, the software tools available, and the size of the dataset (Manyika et al., 2011). Globally, the rise of big data has had immense implications for voter data privacy, given the vast amounts of personal information collected and the lack of transparency and regulatory mechanisms in place to control its dispersion. In 2016-2018, the Cambridge

Analytica Scandal transpired where Facebook data on voters was allegedly misused during the Brexit referendum and the US presidential Elections (Boldyreva, 2018). The case involved non-consensual sharing of Facebook users' personal information which eventually ended up with Cambridge Analytica, a company focusing on big data analytics. In 2015, two American political candidates were associated with the organisation, Ted Cruz and Ben Carson (Boldyreva, 2018), and later in mid-March 2018, the data consulting firm was exposed in its extra-judicial dealings with the Trump campaign as well, where the company harvested more than 50 million Facebook profiles without consent and legal justification. These profiles would later be catalogued into psychological profiles, allowing Analytica to build an algorithm that skewed news results in Facebook users' news feed. This move was not only illegal, but also aimed to and was successful at significantly influencing the result of the US election (Ünver, 2018).

The campaigning period leading up to the recent elections in India provides an interesting perspective into how digitisation of election processes has resulted in the misuse and exploitation of personal data.

THE INTERSECTION OF PRIVACY AND POLITICS: VOTER DATA PRIVACY IN ELECTIONS

Electoral bodies across the world are increasingly employing digital technologies to ensure transparency and more efficient voting processes. This has resulted in increased use of digital technologies during elections, most commonly in the form of digitised voter rolls and electronic voting. Estonia has been the first country to introduce internet voting (Dad and Khan, 2023) by developing a web-based election information system for electoral processes, called the I-Voting system. It covers a wide range of tasks such as registering candidates, managing voting operations, determining results and turnout, and sharing any relevant election related information with the public. Estonia's information systems are mainly populated by election commissions and foreign diplomatic missions responsible for organising the elections. These are also interlinked with other databases, such as the population register and the commercial register, which include data concerning members of political parties (Community of Democracies, 2022). Since its implementation in 2007, it has received praise for its efficiency and use of technology to simplify what can be a complicated process otherwise. Nevertheless, it has received criticism by experts for being vulnerable to internal and external threats, which may compromise the integrity of the system and voter data - such as malware. However, the Estonian government has responded to this critique by consistently upgrading its systems, refining for greater transparency and security (Nurse et al., 2017).

Estonia is a great example of how integration of big data and digital tools can revolutionise electoral processes, especially when governments and institutions prioritise citizen wellbeing. As digital technologies become an established part of modern campaigning techniques, it is important to acknowledge the risks along with the benefits. To effectively do so, and to design systems that account for said risk and benefits, it is important to first understand the complexity of the electoral process, the role digitisation can play, and the importance of keeping data secure from external and internal threats.

Case Study: India's Aadhaar—Elections, Data, and the Privacy Tightrope

In Bengaluru, India, political parties were recently found distributing voter slips via WhatsApp, containing detailed personal information such as voter ID numbers and booth details. Voters reported receiving theirs and their family members voter ID numbers and booth details on WhatsApp. The message also requested them to support a specific candidate from the Aam Aadmi Party. An organisation tasked with voter verification, Chilume Trust, was also found to be collecting Aadhaar card details and voter preferences from people, in violation of the Election Commission Guidelines. A glance at the broader issue shows that voter databases have been accessed by parties (Shree, 2023).

Despite the recognition of privacy as a fundamental right under the Indian Constitution, the Bengaluru case reveals significant legal ambiguities and gaps within the election process - especially when it comes to how voter data is handled. The case demonstrates how voter data, disseminated through platforms like WhatsApp, can be exploited for micro-targeting by political parties. This not only raises ethical questions but also exposes vulnerabilities in digital security that allow such breaches to occur. The technological facilitation of these breaches highlights the critical need for robust digital security measures to protect voter data from unauthorised access and misuse.

Furthermore, the misuse of voter data for micro-targeting has significant implications for electoral integrity. By linking voter slips to mobile numbers and disseminating them via WhatsApp, political parties engage in micro-targeting, manipulating voter behaviour. This practice undermines the democratic process, fostering misinformation and polarisation, and eroding public trust in the electoral system. The parallels between such practices in India and similar concerns in Pakistan underscore the regional challenges in protecting voter data and ensuring electoral integrity.

Similarly, Pakistan has experienced its fair share of scandals when it comes to the management of voter data. In a 2012 interview with Imran Khan, Julian Assange, Wikileaks founder, referred to a diplomatic cable where then prime minister Yousaf Raza Gillani and interior minister Rehamn Malik offered to share NADRA's voter data with a UK based front company, International Identity Services. The company had been hired to extract sensitive citizen data across Pakistan. Assange described this as a large-scale theft of private citizen information, directing the conversation towards the lack of accountability and transparency within these institutions, allowing the political elite to exploit the public (World Tomorrow by Wikileaks, 2012) (Raza & DAWN News, 2012) However, NADRA has vehemently denied ever sharing data with any foreign organisation or compromising on the security of citizen data (Qarar & DAWN News, 2017).

More recently, government investigations have revealed that the data of more that 2.7 million Pakistanis has been stolen from the records of the National Database and Registration Authority (NADRA) office over a period of 5 years. It was reported that NADRA offices in three cities, Peshawar, Karachi, and Multan, were involved in the data leak. Allegedly, the data was first sent to Dubai, from where it was later sold to Romania and Argentina - emphasising the seriousness and magnitude of the breach (The Nation, 2024).

The issue of NADRA's vulnerability to data leaks and weak security measures has been raised in the past but gained prominence only after the disclosure of information leak about certain senior military officials. In October 2022, travel records and personal data of General Asim Munir and his family were accessed and leaked by NADRA officers in an attempt to prevent his appointment as the chief of army staff later in the year (EFE, 2024). The response to this was intense with parliament members suggesting that military personnel and the ISI be involved in the investigation and punishment of those involved in the data breach (DAWN News & Nasir, 2023).

Evidently, while digitisation of election processes has enhanced operational efficiency and enabled advanced data analytics, it has also posed risks related to data protection, especially in countries like Pakistan, which lack stable data protection frameworks. The complexity of electoral processes is intensified as political parties and electoral bodies increasingly leverage digital tools for data collection, and the potential for misuse of information—whether through unauthorised access, breaches, or improper use—grows (European Commission, 2021). This raises fundamental concerns about the integrity of electoral processes and the protection of voter rights. Digitising these processes requires careful planning in order to secure sensitive information, prevent hacking, and ensure voter privacy. Regular updates and security audits are essential to mitigate risks like data breaches and unauthorised access, which outdated systems are easily susceptible to. Effective management must prioritise data privacy. Data privacy involves protecting individuals' personal information from unauthorised access and misuse. In the context of elections, this encompasses safeguarding sensitive voter data, including names, addresses, contact details, and voting preferences (Karjian, 2018).

To gain greater insight on Pakistan's data privacy frameworks, it is important to understand how data is managed in the country, and what frameworks currently exist for protecting citizen data.

DATA PROTECTION IN PAKISTAN: THE ROLE OF ECP, NADRA, AND TELECOM COMPANIES IN MANAGING VOTER DATA

Pakistan's citizen data is collected and managed by the National Database and Registration Authority (NADRA), an autonomous agency formed in 2000. During elections, to ensure smooth electoral processes, it works with the Election Commission of Pakistan (ECP) by sharing relevant and updated voter data lists. In Pakistan, governmental bodies like NADRA and ECP handle vast amounts of sensitive information, which emphasises the need for robust data protection measures. Existing legal provisions such as the Data Protection Bill 2023, Elections Act 2017 and Election Rules 2017 give us greater insight into the regulation of electoral processes and how voter and election-related data is collected, transferred, and stored.

To understand the importance of data privacy, it is first essential to understand how citizen data is collected, managed and stored in Pakistan, especially around elections. To put it simply, NADRA collects citizen data, and then shares it with ECP, which is responsible for creating and updating electoral rolls. Section 25 of the Elections Act 2017 outlines the role of the National Database and Registration Authority (NADRA) in transmitting voter data to the Election Commission of Pakistan (ECP) in greater detail. An interview with the Ex-Chairman of NADRA, provided more insight on Section 25 and NADRA's role in transmitting and handling voter data. He specified that only data relevant to the voter lists, such as name, CNIC number, date of birth, and address is shared with ECP. This is sanctioned/mandated under Section 25 of Pakistan's Election Act, 2017. When NADRA issues a new National Identity Card (NIC) to a citizen, it is required to transmit the relevant data to the ECP. This data includes the cardholder's permanent or temporary address, as specified by the individual during the application process. The purpose of this data transfer is to ensure that the cardholder is registered as a voter in the correct electoral area. Moreover, NADRA is also tasked with providing the ECP with information about any changes to or cancellations of National Identity Cards, details about deceased voters, and any other data that the ECP might require for maintaining accurate electoral rolls. This ensures that the voter registry is constantly updated, reflecting any changes in voter status.The ECP, upon receiving this data from NADRA, forwards it to the relevant Registration Officers, who are responsible for making the necessary updates or corrections to the electoral rolls. This process ensures that the electoral roll remains accurate and up to date, thereby maintaining the integrity of the electoral process.

Similarly, under Section 39 of the Election Rules 2017, NADRA electronically transmits data of all newly registered ID cards, including the person's preferred address and information on whether they want to be registered as a voter. This data is transmitted to the ECP via Form-18[4], on a monthly basis - or as required by the commission. Form-18 is used to officially request corrections or updates to the electoral roll to ensure accuracy. Additionally, Section 44 of the Elections Act 2017 specifies the reciprocal communication of voter information from the ECP to NADRA. When there is a change in a voter's address or any other modification in their registration details, this information is communicated by the Registration Officer to NADRA via the ECP. This ensures that NADRA's records are updated accordingly, maintaining consistency between the national database and the electoral rolls. According to the Ex-chairman of NADRA, the automatic transmission of voter related data between NADRA and ECP, including new registrations and updates ensures that the commission receives accurate and timely information. NADRA shares this new data on a monthly basis, allowing ECP to verify the data according to district and maintain up to date electoral rolls. This system of data sharing promotes transparency and minimises errors in voter registration, ensuring a more reliable electoral process. The ECP also conducts its own verification process to further ensure the accuracy of voter lists. However, these also raise significant concerns about voter data privacy. There lies an implication of responsibility on the part of NADRA and the ECP to implement robust mechanisms to protect citizen data, and further inform citizens about how their data is being used and safeguarded. The effectiveness of these measures is crucial in protecting the privacy of voters and maintaining trust in the electoral system.

Additionally, according to Section 45(2) of the Election Rules 2017, copies of the published electoral roll are stored in locations designated by the ECP. These copies are available for sale to anyone who wants to apply - at the cost of two rupees per page for the hard copy, along with additional charges for photocopies. Political party candidates and their agents are entitled to obtain hard copies as well as searchable digital copies of the electoral roll with photographs of the voters in line with Section 79. The hardcopy must be provided at the cost of five rupees per page, plus the additional expenses incurred for photocopying. Additionally, the digital copy will be available at ten rupees per page.

Candidates and agents applying for the digital copy must also submit Form-24[5] to the registration officer, providing an undertaking that they will under no circumstances compromise the security or integrity of the electoral data. They must also pledge not to misuse, publish, or share information contained in the obtained electoral rolls in any form. Breach of this undertaking will result in proceedings under 195 for disclosing protected information.

4 Available on page 144 of Election Rules 2017

5 Available on page 157 of Election Rules 2017

Looking more closely at the 2024 election in Pakistan, where voters reported to receive normal as well as pre-recorded phone calls from political party officials and representatives soliciting for support, an important question arose - how did these parties retrieve personal data such as phone numbers? The election rules and Elections Act 2017 confirm that voter data was legally retrievable through the ECP. However, that data was not supposed to include phone numbers of the voters. Then how were political parties able to contact voters with information about their exact names, cities, and polling stations? Later, in the analysis section we will see that many political party candidates were reluctant to share too much information about the data retrieval and storage methods their parties employed. However, according to Digital Rights Monitor (2023) and Abbasi (2024), there are entire websites online that allow users to enter a phone number and reveal someone's CNIC details (and vice versa). When brought to the attention of authorities, at least one website was subsequently banned in the country - but remained easily accessible via a VPN. Lack of necessary action against unethical exploitation of citizen data seems to be a recurrent issue. In 2019, it was noticed that the buying and selling of NADRA and SIM data in public groups online was increasingly becoming a common practice in Pakistan. Due to weak data protection frameworks, the people behind these schemes faced zero to no consequences, and you can often find these groups operating on Facebook. These groups sell everything from family trees, with pictures, call histories of individuals, to lists of numbers of various telecom service subscribers (Abbasi & DAWN, 2019).

Additionally, on the orders of the Pakistan Telecommunication Authority (PTA), telecom companies operating in Pakistan are complicit in operating a mass surveillance system, Lawful Intercept Management System (LIMS), which allows the interception of records and data of its customers. There are no legal procedures or regulations to safeguard customers from this, neither do they have the option to withdraw consent (Abbas, 2024). In July 2024, the High Court learned that LIMS was in place during an audio leak case involving Bushra Bibi, wife of imprisoned former Prime Minister Imran Khan.

Under the given circumstances, the need for stringent data protection laws is greater than ever. Over the years, more than three drafts of the Data Protection Bill have been proposed however meaningful progress is yet to be made. To gain a better understanding of the shortcomings of Pakistan's Data Protection Bill 2023, and in return highlight the necessity for improvement, in the next section we will analyse the bill in detail.

DATA PROTECTION BILL 2023

Pakistan's Personal Data Protection Bill 2023 (PDPB) was proposed by the Ministry of Information Technology and Telecommunications (MoITT) with the hope that it could regulate the collection, processing, use, transfer, and disclosure of personal data while simultaneously providing additional data protection, including against violations regarding a person's data privacy. Unfortunately, there are certain factors that indicate that the bill falls short in addressing certain data safety concerns that it initially aimed to address.

Certain sections of the bill, such as Section 15(a)(viii), allow for exceptions in the processing of sensitive and critical personal data under court orders. While such exceptions are necessary for judicial procedures, it is essential that they align with the fundamental right to privacy guaranteed by Article 14 of the Constitution of Pakistan. This provision underscores the necessity for rigorous protection of voter data, even when it is processed under judicial authority. Insufficient privacy safeguards in these contexts could lead to the misuse of voter information within legal settings, compromising electoral integrity.

The bill also seeks to establish the right to access (Section 16), the right to erasure (Section 26), and the right to data portability (Section 29). However, practical limitations and shortcomings may undermine the effectiveness of these rights. For example, Section 16(3) imposes a fee for accessing personal data. Sections 51 and 54, which outline the complaint process and rule-making powers, further impose fees for filing complaints, possibly deterring individuals from reporting data breaches and violations and even reviewing their own personal information. Furthermore, Section 26 stipulates a 14-day timeframe for data erasure, which may be insufficient for addressing concerns about the timely removal of personal data. A more stringent time frame could enhance protection for voters' privacy and ensure that their data is not retained longer than necessary. Section 29(6) introduces a public interest exception to data portability. Without proper regulation, this exception could lead to the misuse of voter data. It is important that this section includes specific parameters to balance public interest with individual rights, similar to the safeguards established under the General Data Protection Regulation (GDPR). Additionally, any automated decision-making involving voter data must be transparent and free from discriminatory practices.

Moreover, Section 31 mandates data localisation, requiring that critical personal data be processed within Pakistan. This provision puts a great demand on the country's infrastructure and data handling policies, which need to be adequate to make processing and securing voter data an efficient process. Section 32's framework for cross-border data transfers diminishes the necessity for explicit consent from data subjects. It is essential to ensure that voter data

is transferred only with clear, informed consent to uphold privacy and trust. The lack of transparency regarding the Commission's conditions for data transfer complicates this issue, potentially leading to broader and less controlled data-sharing practices.

Additional loopholes in Section 34 provide exemptions for data collection related to research and statistics, particularly in Section 34(2)(f), which gives broad exemptions for 'journalistic purposes' and can lead to severe exploitation of personal data for commercial or political purposes if not properly regulated. Sections 35, 37, 43, and 47 address the independence and authority of the Commission. Provisions granting extensive powers to the Federal Government and imposing constraints on the Commission's autonomy could weaken its capacity to effectively oversee data protection.

It is apparent that the PDPB has significant implications for voter data privacy. While it introduces crucial protections and rights, several provisions require refinement to prevent potential misuse and ensure robust privacy safeguards. Addressing these concerns is imperative for maintaining the integrity and confidentiality of voter data, fostering public trust, and aligning with international best practices in data protection.

By comparing the data protection frameworks in other countries in the region such as India, Sri Lanka, and Malaysia - who also went through an election cycle in the past year - we can gain greater insight into the shortcomings of our own legislations.

DATA PROTECTION FRAMEWORKS: A REGIONAL COMPARISON

India

Both India's Digital Personal Data Protection Act (DPDPA) and Pakistan's PDPB illustrate the global influence of the General Data Protection Regulation (GDPR), implemented by the EU. Nevertheless, the adaptation of these principles in India and Pakistan reveals divergent approaches and challenges, particularly concerning voter data privacy. Key differences emerge between the definitions and scope of the DPDPA and the PDPB. The DPDPA's definition of 'legitimate interest' as a legal basis for processing personal data aligns with the GDPR but can be criticised for its broadness, which may permit extensive data processing without sufficient safeguards for data subjects' rights. The bill also clearly delineates the law's territorial applicability, addressing data transfers and the obligations of foreign entities operating within India (PRS Legislative Research, 2023). Conversely, the PDPB faces similar criticisms but could be seen

as having an even more ambiguous scope, particularly concerning regions like Gilgit-Baltistan and Azad Jammu & Kashmir, complicating its application and enforcement (Dawn, 2023).

The DPDPA emphasises the necessity of obtaining explicit consent from data subjects prior to data processing. The mechanism for securing consent is well-structured, and exceptions are narrowly defined, focusing on legitimate business interests or legal obligations. While the PDPB similarly mandates consent for data processing, it includes exceptions that could undermine data subject protections. Although the PDPB requires data controllers to cease processing upon consent revocation, it permits extended timeframes that, if not strictly regulated, could prove problematic (Koehnke, 2022). Moreover, the bill's provisions on notifying data subjects lack specificity, potentially leading to delays and inconsistencies in data processing, thus affecting data privacy (Dawn, 2023).

The DPDPA grants robust data subject rights, including access to, correction of, and erasure of personal data. It introduces a comprehensive framework for data portability and automated processing, ensuring that data subjects retain control over their data. Additionally, the act stipulates clear penalties for non-compliance and establishes a structured grievance redressal mechanism (PRS Legislative Research, 2023). The PDPB offers similar rights but with certain limitations. For instance, the bill imposes fees for accessing personal data, potentially hindering individuals from exercising their rights. Concerns have also been raised about the timeframe for data erasure, which is considered too lenient. The right to data portability is restricted by broad exceptions, potentially diminishing the effectiveness of data protection (Koehnke, 2022). Regarding cross-border data transfers, both the DPDPA and the PDPB state that sensitive data, including information on an individual's health, sexual orientation, biometric data, and other personal details, may be shared only if other nations offer adequate protection according to appropriate regulatory standards. Both bills prohibit the transfer of critical data outside their respective countries. While the DPDPA defines critical data as relating to national security, the PDPB's definition is less clear, and their emphasis on data localisation, particularly concerning critical data, raises concerns due to the significant strain it may place on Pakistan's infrastructure, economy, and energy sectors (Kapoor & Mukherjee, 2023).

Lastly, the DPDPA provides stringent controls for processing sensitive and critical data, including specific conditions for legal exceptions. It aligns with GDPR principles by ensuring that any exceptions are proportionate and respect the data subject's fundamental rights (PRS Legislative Research, 2023). The PDPB, on the other hand, includes relatively broad exceptions when it comes to processing similar types of data, which may not respect the rights of the data subjects to an appropriate extent. This could compromise data protection and lead to huge implications when enforcing laws when it comes to voter data privacy (Koehnke, 2022).

In summary, the DPDPA appears to be more closely aligned with international standards, offering clearer definitions, stricter consent requirements, and stronger data subject rights. In

comparison, the PDPB's vague terminology and emphasis on data localisation may lead to weaker protection for voter data in Pakistan. This concern is echoed in India with the introduction of the Digital Personal Data Protection Bill 2023, which marks a significant step towards ensuring that personal data, including electoral data, is managed with the utmost care. India's Digital Personal Data Protection Bill 2023 mandates that companies, banks, and government agencies disclose the information they collect, how it is stored, and with whom it is shared. The bill introduces severe penalties for violations, including fines and potential platform blocking, underscoring the importance of transparency and accountability (Kapoor & Mukherjee, 2023). Such stringent legal frameworks serve as a model for other countries, including Pakistan, where the integrity of electoral data and the protection of citizens' personal information are paramount (Dawn, 2023).

Sri Lanka

Pakistan and Sri Lanka have markedly different approaches to data protection legislation. Pakistan's PDPB 2023 is still in its draft stage, whereas Sri Lanka has made significant progress with the enactment of its Personal Data Protection Act (PDPA). The PDPA is inspired by the European Union's GDPR and applies to both domestic and international data processing involving Sri Lankan citizens. Its phased implementation allows data controllers and processors time to comply with the new legal framework, ensuring a smooth transition (DLA Piper, n.d.).

Pakistan's Prevention of Electronic Crimes Act (PECA) 2016 and its proposed PDPB differ greatly in clarity and scope compared to Sri Lanka's PDPA. PECA vaguely defines personal data as "identity information," which lacks the specificity needed to address modern data protection needs, such as distinguishing between personal and sensitive personal data. On the other hand, Pakistan's PDPB offers more detailed definitions, aligning with international standards by including anonymisation and pseudonymization, which are essential for modern privacy regulations (DLA Piper, n.d.).

Sri Lanka's PDPA provides comprehensive definitions similar to those in the GDPR. It defines personal data as any information that can identify an individual, either directly or indirectly, and also introduces special categories of sensitive data, such as racial or political information (Data Protection Act, No. 9 of 2022, 2022). These detailed definitions help ensure stronger protection, something that Pakistan's current and proposed laws have yet to fully achieve.

The governance structures for data protection in both countries are also distinct. Under PECA, Pakistan lacks a dedicated data protection authority, with the Federal Investigation Agency (FIA) and the Pakistan Telecommunication Authority (PTA) focusing more on cybercrime than comprehensive data protection. However, the PDPB proposes creating a National Commission for Personal Data Protection, which would regulate and enforce data protection once the bill becomes law (DLA Piper, n.d.). In contrast, Sri Lanka has already established a Data Protection

Authority under its PDPA, which wields significant regulatory power, including issuing guidelines, investigating complaints, and imposing fines for non-compliance.

Neither Pakistan nor Sri Lanka currently have mandatory registration requirements under their data protection laws. In Pakistan, the proposed National Commission could introduce such requirements once the PDPB is enacted. Sri Lanka's PDPA, while not mandating registration, grants its Data Protection Authority the power to establish future registration rules and requires controllers and processors to publicise the contact details of their Data Protection Officers (DPOs) (Data Protection Act, No. 9 of 2022, 2022).

The role of DPOs also highlights the maturity of each country's data protection framework. Pakistan does not yet require the appointment of DPOs, although the PDPB acknowledges the need for them once it becomes law. Sri Lanka's PDPA, however, already mandates that certain entities appoint a DPO with specific qualifications and responsibilities, reflecting its commitment to best practices in data protection (DLA Piper, n.d.).

Regarding the collection and processing of personal data, Pakistan's PECA contains limited provisions, primarily focusing on the unauthorised use of identity information. The PDPB is expected to expand these by introducing obligations for data controllers, including notifying individuals about the purpose and legal basis for processing their data. Sri Lanka's PDPA, influenced by the GDPR, adopts a more comprehensive approach, establishing clear principles for lawful, fair, and transparent data processing, as well as stricter regulations for handling sensitive information (Data Protection Act, No. 9 of 2022, 2022).

In terms of cross-border data transfers, Pakistan's current framework is somewhat limited, primarily focusing on prohibiting unauthorised transfers of identity information. The PDPB is expected to provide a more robust approach to data sovereignty. On the other hand, Sri Lanka's PDPA requires either an appropriate decision for international data transfers or stringent safeguards in the absence of such decisions, aligning with international standards (Data Protection Act, No. 9 of 2022, 2022).

In relation to data security, PECA lacks specific data protection measures, relying instead on sector-specific regulations. The PDPB is anticipated to introduce clearer data security standards. The PDPA, however, mandates that data controllers and processors implement appropriate security measures, such as encryption, reflecting a proactive stance on data security (Data Protection Act, No. 9 of 2022, 2022).

Concerning breach notifications, PECA does not currently require breach reporting, though the PDPB will introduce a requirement for notification within 72 hours of a breach. Sri Lanka's PDPA has similar breach notification requirements, although further details on enforcement are awaited (Data Protection Act, No. 9 of 2022, 2022).

The enforcement of data protection laws also varies between the two countries. Pakistan relies on its courts and sector-specific bodies to address data-related issues under PECA, while the PDPB would establish a dedicated authority for enforcement. PDPA, in contrast, grants comprehensive enforcement powers to its Data Protection Authority, including the ability to impose penalties and conduct investigations (Data Protection Act, No. 9 of 2022, 2022).

In electronic marketing, Pakistan's PECA addresses spamming but lacks a comprehensive framework. The PDPA requires clear consent for marketing messages and prohibits the use of legitimate interest as a basis for sending unsolicited communications (DLA Piper, n.d.).

Finally, in terms of online privacy, PECA criminalises unauthorised access to data, while the draft e-Safety Bill 2023 aims to introduce further online privacy regulations. The PDPA does not specifically address online privacy tools like cookies but ensures general data protection rights apply (DLA Piper, n.d.).

In summary, Sri Lanka's PDPA reflects a more comprehensive and proactive approach to data protection than Pakistan's existing or proposed laws, aligning closely with international standards and emphasising stronger protections for individuals' data.

Malaysia

Pakistan's data protection framework is also less developed in comparison to Malaysia's. As previously mentioned, Pakistan's bill remains in the draft stage, whereas Malaysia has already established a robust legal framework with the Personal Data Protection Act (PDPA) 2010, which came into force in 2013. The PDPA governs the processing of personal data, particularly in commercial transactions, and is currently being revised to strengthen its provisions, reflecting Malaysia's commitment to staying ahead of technological developments (PrivacyWorld, 2024).

The definitions of personal and sensitive data in both countries illustrate key differences in their legal frameworks. Under PECA 2016, Pakistan defines "personal data" broadly as identity information but makes no distinction between personal and sensitive data. The draft PDPB aims to address this by providing clear definitions of both personal and sensitive data, recognising critical categories such as health and financial information (DLA Piper, n.d.). Malaysia's PDPA, however, already contains comprehensive definitions of personal and sensitive data, offering broader protections for individuals. Under the PDPA, sensitive personal data includes information related to health, political opinions, religious beliefs, and criminal records, making Malaysia's framework more detailed and protective of privacy than Pakistan's current laws.

In terms of data protection authorities, Pakistan does not yet have a dedicated body overseeing data privacy. The FIA and PTA, operating under PECA 2016, focus primarily on cybercrime and telecommunications issues rather than comprehensive data protection. The PDPB proposes

the establishment of a National Commission for Personal Data Protection, which would oversee and enforce Pakistan's data privacy laws (DLA Piper, n.d.). Malaysia, by contrast, has a well-established authority in the form of the Personal Data Protection Commissioner, responsible for enforcing the PDPA, supported by an advisory committee. This gives Malaysia a more structured and effective regulatory framework, with the Commissioner empowered to impose penalties and conduct inspections to ensure compliance (Personal Data Protection Act, 2010). The requirement for data user registration further highlights the contrast between the two countries' approaches. Pakistan currently has no registration requirement under PECA 2016, but the PDPB would introduce such obligations for data controllers and processors once enacted. In Malaysia, several sectors, including banking, healthcare, and communications, are required to register under the PDPA and comply with industry-specific codes of practice. This process enhances accountability and transparency in Malaysia, where data users must renew their registrations and follow detailed guidelines, making the system more stringent compared to Pakistan's current arrangements (DLA Piper, n.d.).

The approach to consent for data collection and processing also differs significantly between the two countries. Pakistan's PECA 2016 offers limited guidance on consent, focusing instead on criminalising unauthorised access to personal data. The PDPB, however, aims to introduce a more detailed framework, requiring explicit consent from individuals and granting them the right to be informed about the collection, processing, and retention of their data (DLA Piper, n.d.). In Malaysia, the PDPA mandates that data users must obtain consent before processing personal data, with clear provisions for informing individuals about the purposes of data collection and their right to opt out of direct marketing. This makes Malaysia's legal framework more advanced in terms of protecting individuals' privacy (Personal Data Protection Act, 2010). Cross-border data transfers are another area where the legal frameworks diverge. PECA 2016 prohibits unauthorised transfers of personal data but lacks comprehensive rules for international transfers. The PDPB would improve these provisions by requiring that personal data transferred outside Pakistan be sent only to countries with equivalent data protection standards (DLA Piper, n.d.). In contrast, Malaysia's PDPA restricts the transfer of personal data to jurisdictions outside Malaysia unless those countries have been approved by the Minister. Exceptions are permitted if the data subject consents or other legal conditions are met (Personal Data Protection Act, 2010). Malaysia's system is better aligned with international data protection standards, and ongoing revisions are expected to further enhance its approach to cross-border data transfers (PrivacyWorld, 2024).

In terms of enforcement, Pakistan's current system under PECA 2016 is limited, with the FIA and PTA handling complaints and violations primarily related to cybercrime. The PDPB, however, promises to strengthen enforcement by empowering the National Commission for Personal Data Protection to investigate breaches and impose penalties. Malaysia's enforcement

mechanisms are more established, with the Personal Data Protection Commissioner overseeing compliance, conducting audits, and issuing penalties for breaches. The PDPA includes provisions for criminal liability, fines, and imprisonment for non-compliance, giving Malaysia a more robust enforcement regime (Personal Data Protection Act, 2010).

In summary, Malaysia has developed a more comprehensive and mature data protection framework compared to Pakistan. The PDPA provides detailed protections for personal data, with a clear regulatory authority and stringent requirements for data users. Meanwhile, Pakistan is still in the process of developing its legal framework through the PDPB, which shows promise but will require substantial legal and institutional development to reach a similar level of protection. In the context of voter data privacy, Malaysia's system offers stronger safeguards, thanks to its established definitions, regulatory oversight, and enforcement mechanisms. Pakistan's evolving framework holds potential, but significant progress is needed to ensure comparable levels of protection (DLA Piper, n.d.).

FINDINGS AND ANALYSIS

The comparison of Pakistan's Data Protection Bill indicates that while legal frameworks in Pakistan aim to establish guidelines for safeguarding private citizen data, the implementation and enforcement, as well as blatant loopholes, remain critical areas of concern. We have established up till now that this is especially true in the context of political campaigns, where an increased use of big data has had significant implications on voter privacy in countries like India, and through cases such as the Cambridge Analytica scandal. In the following section, through data collected via surveys and interviews, we analyse the perceptions and experiences around the lack of functional legal provisions, data breaches, and data-driven political campaigning.

Data-Driven Political Campaigns and Data Breaches in Pakistan: Implications on Voter Data Privacy and Perspectives from the 2024 Elections

During the general elections held in February 2024, concerns around voter data privacy were heightened due to previously reported incidents of data breaches, and an observable increase in the use of voter data for election campaigning by political parties. Weak data protection laws, and inadequate implementation of rules and regulations when it comes to data sharing, and data breaches exacerbated the problem. To gain further insight on data security mechanisms and data breaches within NADRA, we delved deeper into our conversation with the Ex-chairman of NADRA, X. He shared several key insights regarding NADRA's approach to data breaches and security protocols, highlighting the organisation's evolving strategies and shortfalls when it comes to protecting citizen data. He explained that data breaches within NADRA in actuality

are quite difficult to execute due to stringent internal controls. Access to an individual's data requires the authorised person to possess the citizen's ID card number, restricting unauthorised access to a significant extent. However, X stated that there have been incidents in the past where it was discovered that the personal data of members of his family had been accessed by NADRA employees 24 times without authorization. This prompted action, including the dismissal of 325 employees for unauthorised data access, as well as the issuance of over 50 electronic letters to NADRA employees to educate them regarding protecting citizens data and privacy, penalties of unauthorised access, and warnings for employees who access data without authorisation.

During his tenure, X introduced an initiative to enhance data security by rolling out a comprehensive log of all NADRA transactions, allowing audits of data access. This auditing system showed to be an effective tool in identifying those responsible for breaches - however, it remains unclear whether it is still in use.

X also emphasised that data breaches are not primarily caused by NADRA employees but third parties and entities, such as telecom companies, who also misuse NADRA's identity verification services, contributing to the problem. This misuse stems from improper storage and monetization of identity data, highlighting the need for stricter regulation of these third parties. While biometric data, including fingerprints and facial recognition, remains uncompromised, other forms of personal data are more vulnerable.

Additionally, NADRA has taken a proactive stance by implementing campaigns to educate the public on how to protect their personal information. They launched the "Ijazat Aap Ki" service in early 2023, which empowers citizens by allowing them to control who can access their data. However, as with other programs that were set up, the current status of this service remains unclear.

X emphasised NADRA’s zero-tolerance policy towards data breaches. He ensured that all reported incidents were thoroughly investigated and resulted in disciplinary actions against involved parties, including employees, complicit in acts of omission and commission. It was also disclosed that the Information Security (IS) department periodically evaluates data security measures and suggests improvements in light of the challenging environment. However, while NADRA has established strong internal measures, the vulnerability often lies in third-party misuse, and stronger regulations are required to mitigate these risks.

The recent data breaches, as well as insights from our interview with X have exposed the vulnerability of citizen information, particularly voter data. Data collected through additional interviews with voters and political candidates showed that the parties which were able to access extensive voter data engaged in tactics like targeted political advertisements and automated phone calls. Several political parties were accused by voters and candidates of

competing parties of accessing voter lists far beyond their constituencies. While these techniques appeared to be effective in mobilising election campaigns, they raised ethical concerns regarding transparency, privacy of voters, as well as around the disruption of a fair playing field for political parties when it comes to contesting in an election.

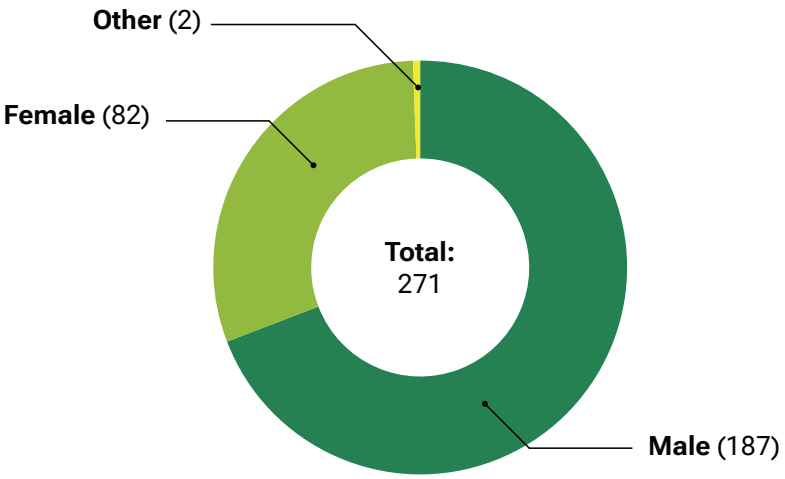
Findings from voter surveys and in-person interviews have provided us greater insight into the impact of data breaches, and data driven political campaigns, and what narrative political candidates hold to justify their tactics.

Demographic Overview

From the 271 participants who filled in the surveys, 69% (187) were male, 30.3% (82) were female, and only 0.7% (2) identified as "other".

Survey Data: Gender

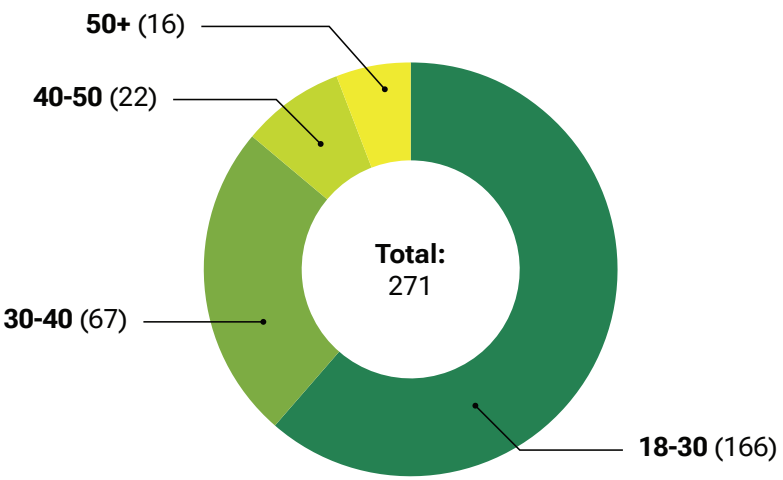
Division of genders in survey responses



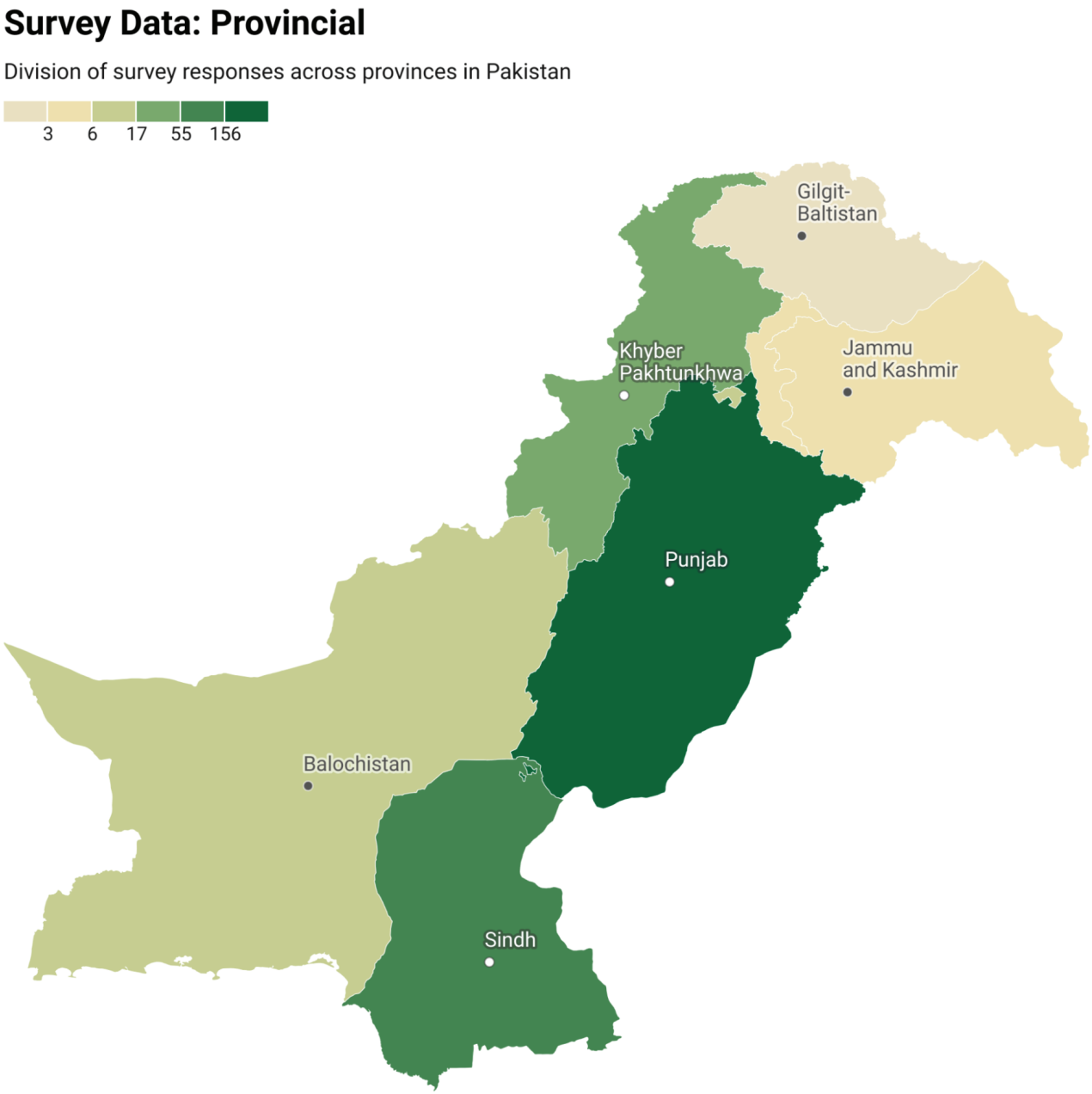
The age distribution showed that 61.25% of the respondents were between the ages of 18-30, 24.7% were between the ages of 30-40, 8.12% were between the ages of 40-50, and 5.9% were above the age of 50.

Survey Data: Age Brackets

Division of age in survey responses



Respondent Distribution: Collection, Scope, and Relevance

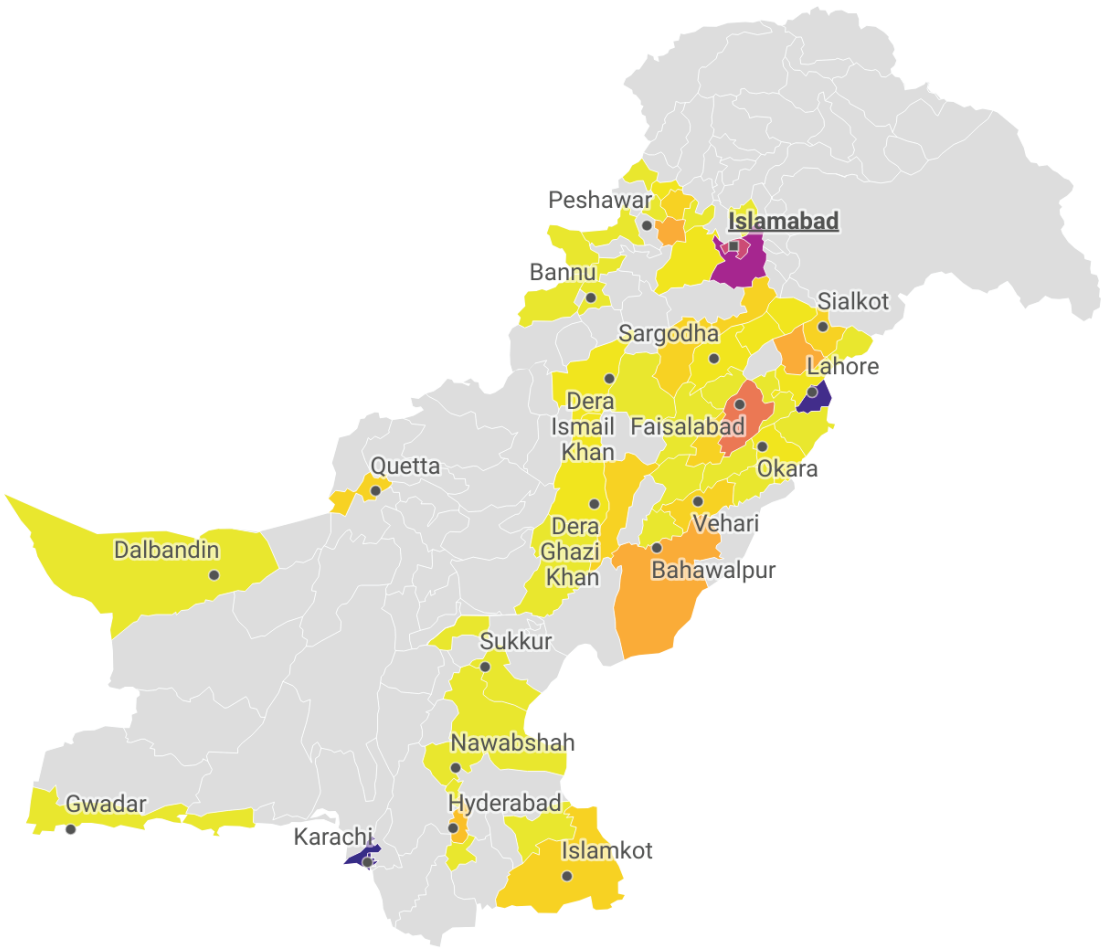


The map shows the spread of surveys collected from across the different provinces in Pakistan. Punjab is in the majority with 57.6% (156 responses), then Sindh with 23.9% (65 responses), followed by Khyber Pakhtunkhwa at 14.4% (39 responses), Balochistan at 2.58% (7 responses), Jammu and Kashmir at 1.11% (3 responses), and lastly Gilgit Baltistan at 0.37% (1 response). This spread falls in line with population and technology spread across Pakistan. Punjab, as the most populous province, houses over half of Pakistan's population (approximately 127

million out of 240 million)[6] and benefits from more robust infrastructure, better access to technology, and higher literacy rates. These factors naturally lead to a higher engagement in surveys and data collection activities. Similarly, Sindh, which includes Karachi—the largest city in Pakistan—also has a high population concentration (around 55 million) and advanced technological penetration, making it more receptive to surveys. In contrast, Balochistan, despite being the largest province by area, is sparsely populated with only about 14.8 million people and lags significantly in technology infrastructure and accessibility. The province's difficult terrain and sociopolitical issues contribute to lower survey responses (Khan et al., 2022). Likewise, Gilgit-Baltistan and Jammu and Kashmir are even more remote and underdeveloped in terms of technology spread, with populations of approximately 1.5 million and 4.5 million, respectively. These regions often face challenges such as limited internet access, rugged terrain, and lower literacy rates, which hinder effective survey participation (Shah et al., 2023).

Survey Data: Districts

Number of survey responses from districts in Pakistan



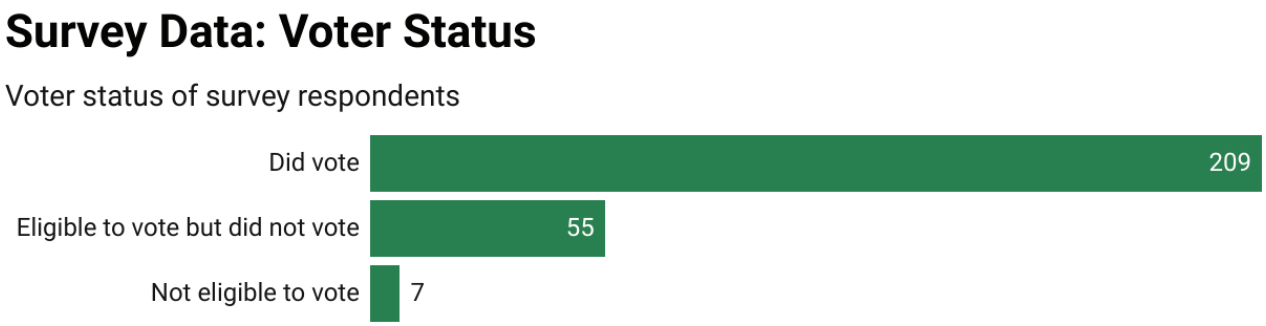
6 As updated on City Population in accordance with the 2023 census.

The district map offers critical insights into Pakistan's digital infrastructure, privacy concerns, and security, as seen through the disparities in survey response rates across various regions. These patterns of participation highlight the broader challenges related to digital literacy, data privacy, and security in voter data collection and electoral processes.

Survey participation is highest in major urban centres like Lahore, Karachi, and Islamabad due to their superior technological infrastructure, better internet connectivity, and higher digital literacy rates. However, concerns about data privacy and security remain, with many citizens in these areas uneasy about potential data misuse in the absence of strong privacy laws. The research report, Doing Digital for Development (2024), by the United Nations Development Programme (UNDP), highlights the tension between digital progress and privacy concerns in Pakistan. With growing digitization of economic and government institutions, a significant amount of sensitive data has been accumulated. Protecting this data, and ensuring transparency about how it is used is paramount to fostering public trust and maintaining accountability (Doing Digital for Development, 2024).

Rural and peripheral areas like Balochistan, Khyber Pakhtunkhwa, and Gilgit-Baltistan exhibit the lowest participation rates due to poor internet access, lower literacy, and deep mistrust of both government and private entities, as supported by reports from Media Matters for Democracy [7] (2022) and The Diplomat [8] (2020). These regions remain politically and technologically marginalised, contributing to their limited engagement in digital surveys and elections.

Survey data showed that 77.12% of the respondents reported to have cast their vote in the General Elections held in February 2024. 20.3% stated that they were not able to or chose not to cast their vote, even though they were eligible. 2.6% reported that they were not eligible to vote yet.



7 See report: Connecting the Disconnected: Mapping Gaps in Digital Access in Pakistan

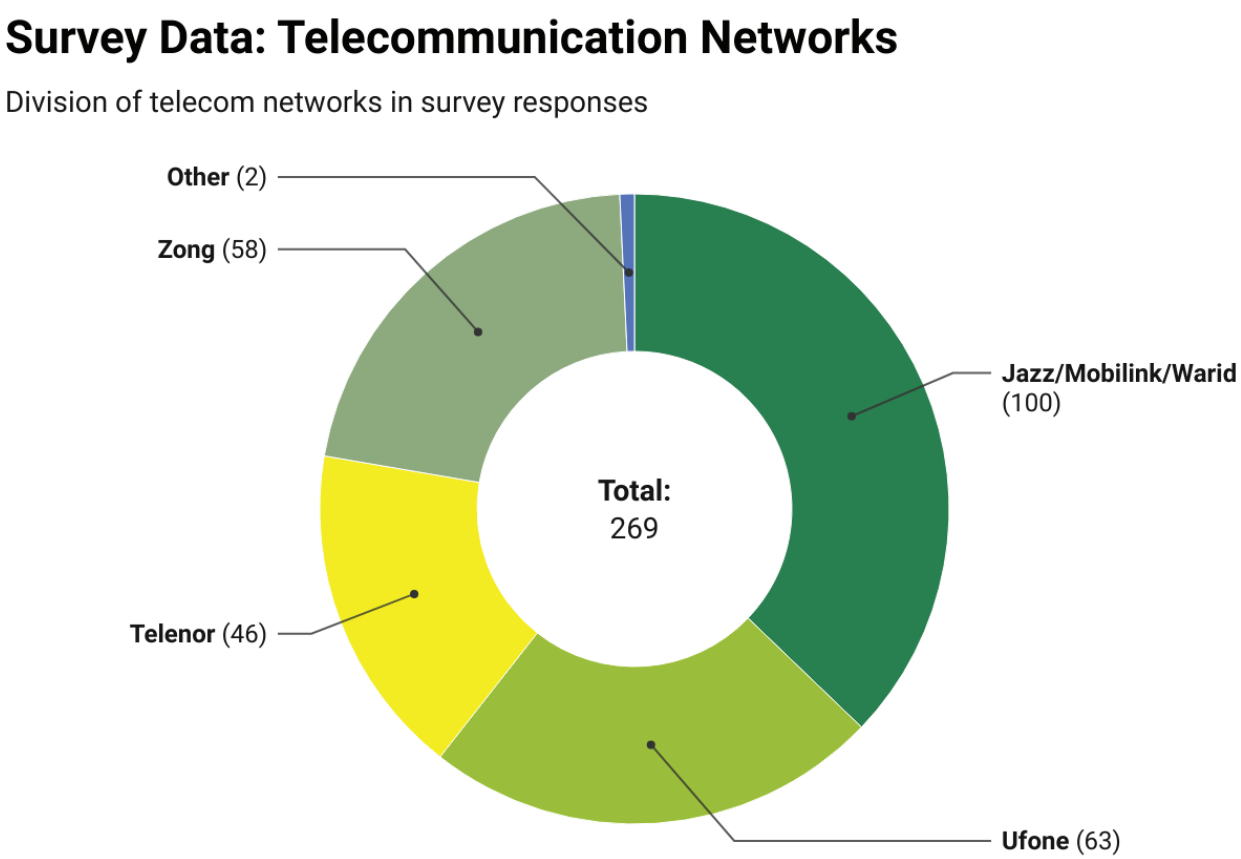
8 See article: Pakistan's Great Digital Divide

As we move forward in our findings and analysis, in order to effectively analyse the collected data, we have organised the results into 11 key themes - (1) Telecom Providers and Data Misuse; (2) Forms of Data Misuse in Political Campaigns; (3) Political Parties Involved in Data Misuse; (4) Perceptions on Data Regulation; (5) Awareness of Data Protection Laws; (6) Tendency to share personal data; (7) General acceptance towards use of AI in electoral contexts; (8)Use of social media; (9) Tools used for election campaigning and retrieval of voter data; (10) Understanding of and willingness to incorporate transparency protocols; (11) Voter Recommendations on Data Privacy.

These themes will be used to guide the discussion, outlining the insights drawn from the surveys, voter interviews, and political candidate interviews.

1. Telecom Providers and Data Misuse

Of the six voters interviewed, three respondents had two SIM cards from different network providers. Five used Ufone, while two used Jazz, and two Zong. From the voter surveys, 100 respondents used Jazz/Mobilink/Warid, 63 used Ufone, 46 Telenor, 58 Zong, with one respondent each using SCOM and STC.



2. Forms of Data Misuse in Political Campaigns

From the survey data, 38.37% (104) reported to have received automated calls, texts, and whatsapp communication from political parties - without having signed up for it prior. When asked if they received calls or messages from political parties regarding casting a vote in their favour, 46.49% (126) participants responded affirmatively.

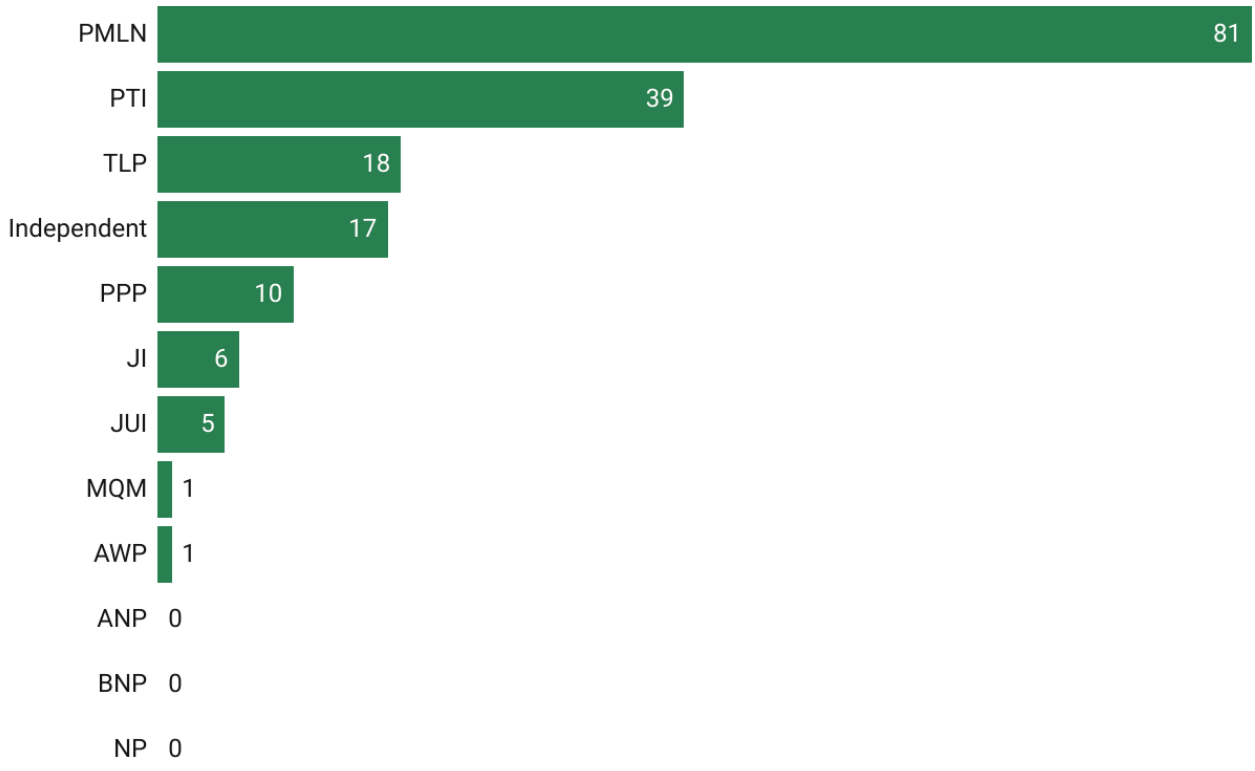
During an interview with a voter, she reported being on the receiving end of multiple forms of outreach from political party representatives as a part of their election campaign. These included automated calls from Nawaz Sharif (PMLN) and Imran Khan (PTI) (Durrani, 2024) (Younus, 2024), as well as voter slips for her and her family, sent via WhatsApp. This was accompanied with a voice note urging them to vote for that specific party. Additionally, two voters received automated calls from Nawaz Sharif, while another voter received physical voter slips from both PPP and PMLN. One voter only received a text, although they did not specify its contents, or the sending party. Only one voter that we interviewed reported to not have received any political outreach through phone calls or voter slips, although he recalled having received both in the 2018 elections.

3. Political Parties Involved in Data Misuse

Out of the six voters interviewed, one did not specify the party that contacted them via SMS. There were four instances of communication from PMLN, three from PTI, and one from PPP (with some voters reporting multiple contacts). This aligns with data from the voter surveys, where 81 respondents identified PMLN as the party that reached out for votes, followed by 39 who were approached by PTI. 18 respondents were reached out to by Tehreek-e-Labbaik Pakistan (TLP). 17 identified independent candidates, 10 identified as PPP, 6 identified as JI, 1 identified as Muttahida Qaumi Movement (MQM), and 1 identified as AWP.

Survey Data: Vote Solicitation

Number of survey respondents identifying the party that tried to solicit their vote

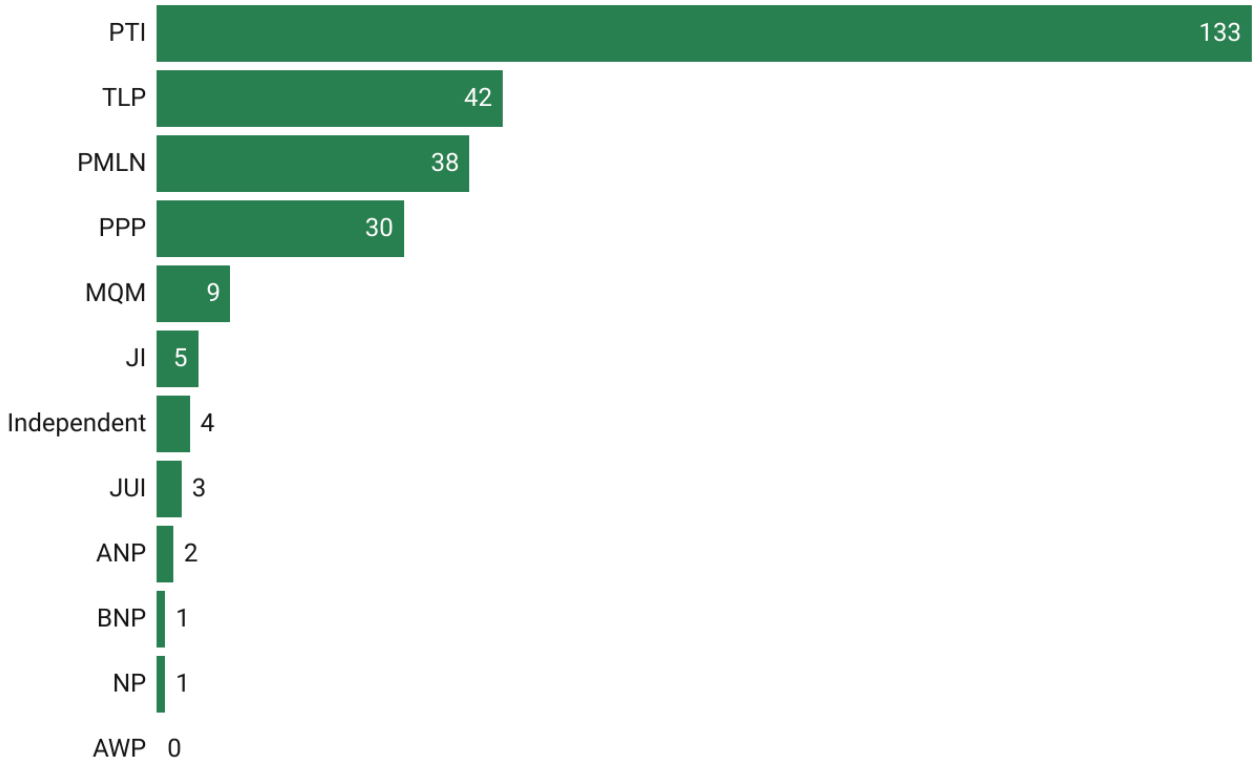


When compared to data on the most prominent political parties in their areas, PTI and TLP were found to be more visible than PMLN. Several factors contribute to this; PTI reportedly led in political advertising on social media platforms, using advanced AI tools to bolster their election campaigns. The party's heavy reliance on social media was partly due to the restrictions placed on them, forcing many of their candidates to run as independents with obscure symbols assigned by the ECP.

In our interview, the PTI member highlighted that the party was forced to rely heavily on social media tools to target local voters and maximise outreach, since traditional campaigning was not an option due to the ban on the party, they had to lean heavily on social media tools to target local voters as well as overseas supporters. Alongside the voter data provided by ECP, PTI also reported to have utilised door-to-door campaigns and social media efforts to run a successful campaign, despite restrictions on rallies and public events.

Survey Data: Political Presence

Number of respondents identifying the most prominent political party in their area



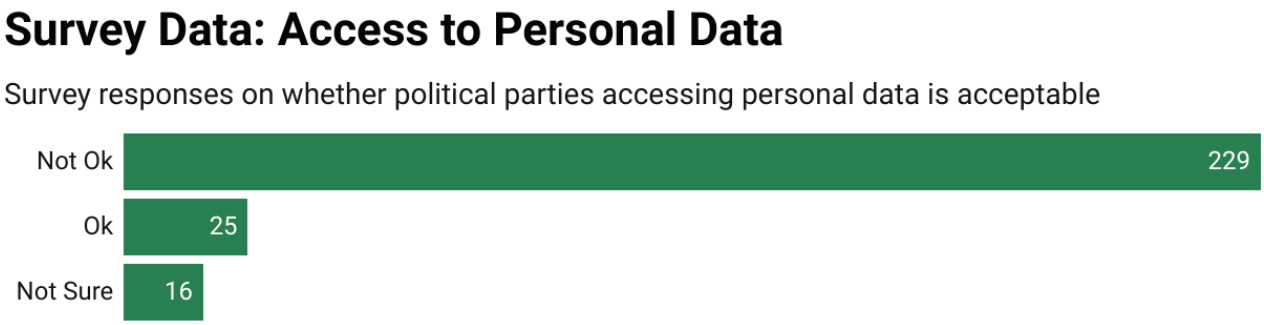
Despite restrictions on traditional campaigning, data collected through surveys showed that PTI was the most prominent political party in their respective areas - indicating that their 'non-traditional' campaigning efforts might have been a factor in garnering public support.

Another interesting aspect of our findings was the claim made by the PPP spokesperson, who claimed that their campaign did not include the use of automated calls. She emphasised her focus on social media, television advertisements, and door-to-door canvassing efforts. However, data from the voter survey contradicted this, with at least two respondents reporting they had received automated calls from party leader Bilawal Bhutto, asking for their support.

This contradiction raises questions about the transparency of political campaign practices, suggesting possible disorganisation within the party or discrepancies between what is officially communicated and what actually occurs during campaigning. It also highlights potential concerns around the respect for voter data privacy, as voters may be targeted without their full awareness or consent.

4. Perceptions on Data Regulation

Several voters voiced concerns about data privacy, expressing unease about the lack of regulation surrounding personal information, especially during and after the election period. From the survey data, 84.5% of respondents expressed that they were not okay with political parties accessing their personal data for political campaigning, 9.2% said they were okay with it, and 5.9% were unsure.



During an interview, a voter expressed their discomfort with access to their data after recounting an incident that highlighted the vulnerabilities in Pakistan's data management system: she reported that following her brother's test results, the family was flooded with advertisements from schools and colleges. She suspected the school board office had sold his data to educational institutions, highlighting how easy it was for private information to be leaked and misused. This voter also raised concerns about how personal information, including phone numbers linked to CNICs, could be exploited by third parties, posing a significant privacy risk.

Several voters were aware that voter data used by political parties during the election likely came from sources such as NADRA or service providers such as mobile companies, even though official voter lists do not include contact numbers. This pointed to the broader issue of telecommunication companies and government institutes being complicit in major citizen data leaks. One voter described this practice as a breach of privacy, as their data, along with detailed personal information, was used without consent.

Voters also recognized the global nature of data privacy challenges, but pointed out that the state of data regulation in Pakistan is particularly weak. One interviewee emphasised the need for improved government policies, noting that even bank accounts and apps were vulnerable to hacks. This voter called for more stringent data privacy training and better enforcement of privacy protections.

Some voters suggested that while security concerns, such as preventing terrorist activities, justify some level of data access by authorities, the sharing of personal data with political parties for campaigning purposes was seen as unethical. This perspective underscores the

need for clearer boundaries between national security measures and the use of data for political purposes.

Lastly, there was widespread scepticism about the implementation of data protection policies in Pakistan. One voter commented on the disparity between official policies and their implementation, stating that data can be easily accessed if one has the means to bribe officials, making Pakistan a "graveyard of policies" in terms of data regulation.

These outlooks highlight a lack of trust in how data is managed, with voters feeling that existing privacy laws are neither adequately enforced nor sufficiently protective, particularly during politically charged events like elections. The findings indicate an urgent need for reform to ensure transparency, accountability, and the ethical use of personal data in political processes.

5. Awareness of Data Protection Laws

The interviews with both voters and politicians revealed varying levels of awareness about data protection laws in Pakistan, highlighting significant gaps in understanding and a general lack of clarity on the legal framework regarding voter data privacy.

Among voters, there was little to no knowledge about formal data protection regulations. One voter expressed that, while they believed there should be laws governing data regulation and privacy, they were unaware of any such rules. They noted that the lack of protections made them hesitant to share personal information, fearing misuse, especially in a context where women are particularly vulnerable to harassment. Another voter shared similar concerns, citing that despite being aware of some cybercrime laws, they had no knowledge of how their personal data could be protected if it were misused.

Some voters had limited awareness of the Data Protection Bill, but expressed confusion regarding its implementation status. One voter mentioned having heard of the bill but had no current information about its progress or effectiveness. Another voter, who had done prior research on data protection, criticised the bill for being vague and leaving many questions unanswered about how data could be shared and used. They also referenced recent incidents, such as the "firewall situation [9]," to illustrate how data is mismanaged in Pakistan.

9 In August 2024, many in Pakistan complained about noticeably slow internet speeds, which the government of Pakistan was reluctant to provide a clear answer for, claiming at first that underwater cables were damaged, and then that people using VPNs to access the internet were to blame. The general consensus, however, is that the slowness is due to the government implementing their own version of China's "Great Firewall" to block "anti-state" material. Though the government had denied the "firewall" or Web Management System (WMS), at first, they confirmed its existence at the end of August 2024. Abassi, S. (2024, September 15). Pakistan's Firewall Explained. *The Express Tribune.* https://tribune.com.pk/story/2494442/pakistans-firewall-explained

On the political front, a similar lack of awareness was observed, although the responses varied slightly depending on the political party. The political candidate from PPP expressed that while she was not aware of any specific data protection laws, she emphasised the importance of regulating how personal data is accessed and used. She described the process of drafting bills and the importance of lobbying for reforms but admitted there was no significant focus on voter data privacy at the parliamentary level. The political candidate from AWP explained that there is no specific law prohibiting the provision of voter data to candidates or political parties. Voter data, such as names, identity card numbers, and addresses, is provided by the ECP on the basis of constituencies and is easily accessible to contesting parties. Since this data is publicly available and tied to constituencies rather than individuals, the candidate argued that it does not infringe on anyone's privacy. Furthermore, the ECP is obligated to provide this data to candidates, and there are no legal restrictions against its distribution.

Additionally, the candidate from PTI, who had an extensive legal background, expressed significant concerns about the allegedly biased actions of the ECP and other institutions, particularly in the context of elections. He was aware of existing legislation aimed at data protection and voter privacy in Pakistan, but emphasised that the real problem lay in the inefficient enforcement of these laws. According to him, manipulative practices like reallocating polling stations and generating inaccurate Form 47 [10] results highlighted the failure of the current legislation. He also criticised the ECP's rejection of electronic voting systems, suggesting that while legal frameworks are in place, they are undermined by inefficient manual processes and corrupt practices, making the legislation ineffective in practice.

However, a representative from JI claimed that while he was not aware of any specific data privacy laws, the party had always respected the boundaries of data privacy and would adhere to any such laws if they existed. He emphasised that their party would never intentionally violate privacy, stressing the importance of ethical practices even in the absence of formal legal frameworks.

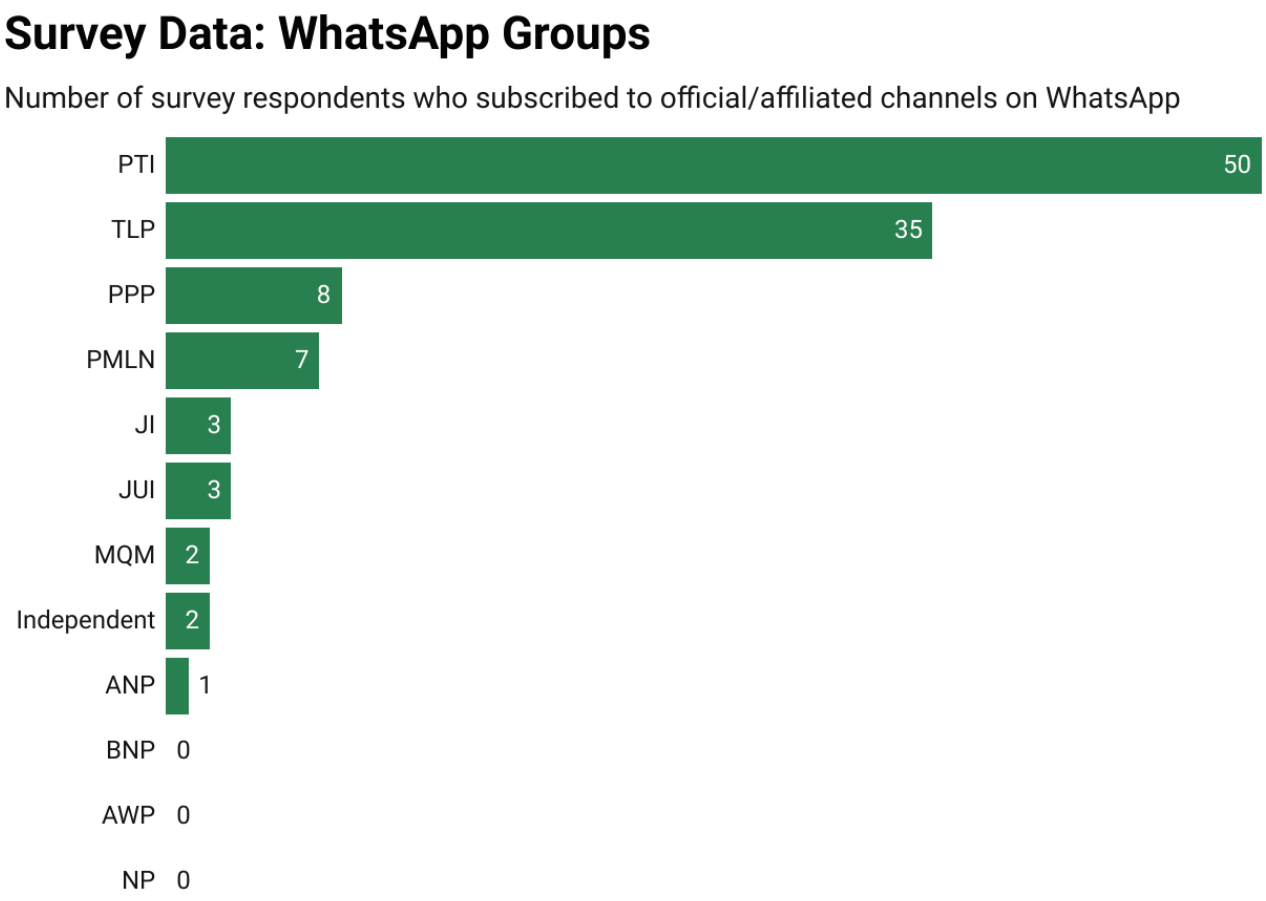
The political candidate from HKP expressed concerns about the easy accessibility of voter data through the Election Commission. He noted that obtaining the voter list, along with digital data files, was relatively straightforward by the Election Commission for a nominal fee— around four rupees per number. The candidate highlighted that for large-scale messaging, such as reaching hundreds of thousands of individuals, the process was simple and did not require

10 Available on page 179 of Election Rules 2017

significant oversight. He expressed concern about the potential misuse of this data by others who might exploit it without requisite understanding of data protection legislation. He also pointed out that many officials within the Election Commission and related offices may lack the technological expertise necessary to handle this data responsibly, raising further apprehensions about the proper use and security of voter information.

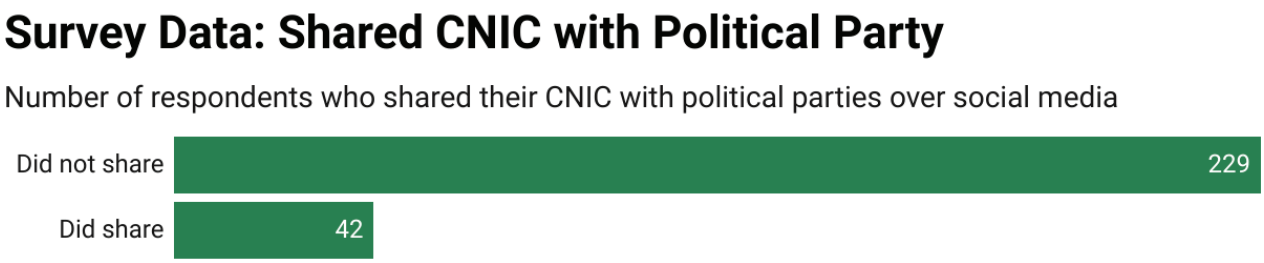
In conclusion, the findings from both voter and politician interviews revealed a concerning gap in awareness about data protection laws in Pakistan. While some individuals were aware of the existence of the Data Protection Bill, the overall lack of clarity and implementation leaves both voters and political actors in a state of uncertainty.

6. Tendency to share personal data



The data collected from the survey highlights two prominent ways in which individuals in Pakistan may be at risk of oversharing personal information online. A significant portion of the survey respondents—111 out of 271 (40.96%)—reported joining WhatsApp groups of various political parties. Additionally, 42 out of 271 (15.49%) respondents disclosed that they shared sensitive information, such as their CNIC numbers, with entities they believed to be political

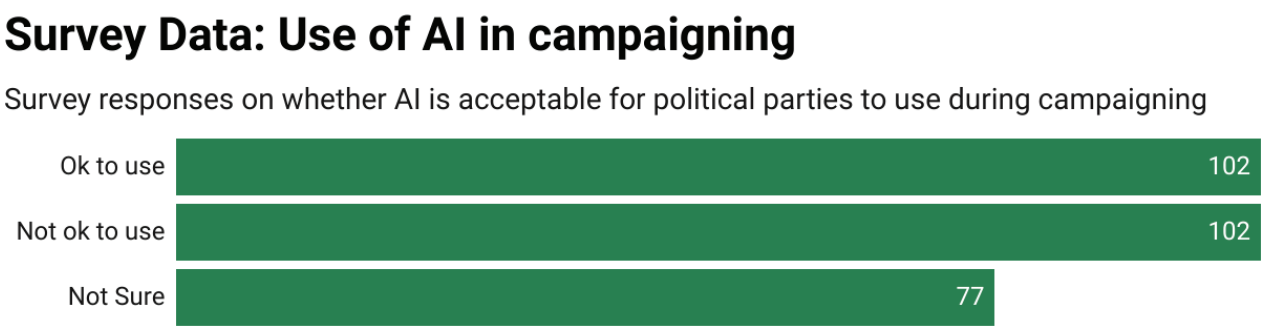
parties operating online. These statistics illustrate a widespread trend of engaging with digital platforms in a manner that leaves personal data exposed to potential misuse.



The tendency to overshare can be traced back to several factors, primarily low digital literacy and a limited understanding of data privacy risks. According to research on students' use of information and communication technologies (ICTs), a significant number of users engage with digital platforms, often for purposes such as entertainment, education, or social interaction, without a clear understanding of the associated privacy risks (Shahid et al., 2022).

The lack of awareness about the implications of sharing personal data is compounded by the weak regulatory framework that exists in Pakistan. Current privacy laws are inadequate to protect users from the potential misuse of their data. Once shared online, personal information such as CNIC numbers can be exploited by malicious actors, with little recourse available to the individuals affected. This vulnerability is particularly concerning in the political realm, where the misuse of personal information can lead to manipulation, coercion, or even voter suppression.

7. General acceptance towards use of AI in electoral contexts



Data from the surveys interestingly showed that people were divided on the acceptability of AI tools employed for political campaigning. 37.1% said it was acceptable to use AI in political campaigns, while 37.1% disagreed with its use. 28.4% were unsure about where they stood on the matter. These results could be attributed to the significant use of artificial intelligence

technologies employed by PTI, who not only used AI to generate voice recordings for automated calls, but also used it for AI generated speeches (The Guardian, 2023). There was also speculation around an article published in The Economist, claimed to be authored by Imran Khan. Concerns arose due to the language used and writing style, instead of the content itself. However, PTI addressed these concerns, denying AI use and claiming that the piece was authored by the PTI Chairman, Imran Khan, who provided the points through meetings and visitations that were later combined into an article (DAWN News, 2024). However, PTI's use of AI and technology allowed supporters a way to connect with him - possibly attributing to the mild approval of AI reflected in our collected data.

8. Use of social media

Across various political parties, social media emerged as a critical tool for election campaigns. Candidates from different political backgrounds emphasised its role in engaging voters, disseminating information, and countering restrictions imposed on traditional campaigning. The PPP candidate highlighted how social media, along with television advertisements, was central to Bilawal Bhutto's campaign in NA-127. She explained that targeted advertising on digital platforms allowed the party to address specific issues important to communities, for example, concerns about a Christian graveyard. These efforts were part of a broader strategy to tailor messages to different voter segments, reflecting the power of digital platforms to reach distinct constituencies effectively.

As reported by the AWP candidate, social media was a crucial tool for outreach and mobilisation, especially given the party's limited financial resources. Platforms like Facebook, Twitter (now X), and Instagram allowed AWP to connect with voters, particularly in areas where traditional campaigning was challenging. The candidate observed a marked increase in the impact of social media compared to previous elections, emphasising its importance in bridging the gap between the party and the electorate.

JI also relied on social media to reach the masses, despite limited resources. The JI candidate noted that the party organised social media training workshops for their workers and used these platforms to spread their manifesto and attract voters. The party's effective use of digital media enabled them to engage voters and promote their election agenda at a broader level than traditional methods would allow.

For PTI, social media played an especially crucial role due to restrictions on public gatherings following the May 9 riots [11], incited by the arrest of party leader, then Prime Minister Imran

11 Read more: A year since Pakistan's May 9 riots: A timeline of political upheaval https://www.aljazeera.com/news/2024/5/9/timeline-a-year-of-ex-pm-imran-khans-arrest-may-9-violence-in-pakistan

Khan. With physical rallies curtailed, the party shifted its focus to social media, where it could still connect with both domestic and overseas voters. The PTI candidate was particularly pleased with the party's effort to effectively use constituency-specific voter data to send voice messages and mobilise support. The candidate expressed pride in the unprecedented use of social media, noting its role in amplifying Imran Khan's message and engaging millions of voters across Pakistan and abroad. Platforms such as Facebook and Instagram were particularly instrumental in reaching voters in areas where on-ground campaigning was restricted.

The candidate from HKP similarly acknowledged the positive impact of social media on their campaign. Although they lacked the financial resources of mainstream parties, social media platforms like TikTok and Facebook allowed them to engage voters, particularly those who could not attend rallies in person. However, the HKP candidate pointed out a challenge: wealthier, more established political parties could outspend smaller parties on social media campaigns, creating a disparity in reach.

In summary, social media emerged as a superior campaigning tool in Pakistan's 2024 elections, allowing both major and minor political parties to engage voters and disseminate their messages, overcoming campaign restrictions where applicable. However, financial inequalities prevented a level playing field as smaller parties struggled to match the spending power of larger political organisations.

9. Tools used for election campaigning and retrieval of voter data

The use of voter data and digital tools varied significantly across political parties during the 2024 elections in Pakistan. All candidates acknowledged the importance of voter data in campaigning, though their methods and resources differed based on party size and financial capacity.

The PPP candidate shared that the party sourced voter lists directly from the ECP and used them to target specific areas through social media advertising. Their campaign employed geofencing for political ads and drew on polling data from organisations like Pulse, alongside other research reports. While they claimed to not have sent out automated calls, they relied heavily on traditional methods, including door-to-door canvassing and word-of-mouth – due to Pakistan's underdeveloped digital infrastructure.

AWP also relied on ECP voter lists for election day operations. They used both physical voter slips and a backup digital application for voter verification, which proved helpful during internet shutdowns. Although they did not use automated calls, the candidate pointed out that larger

parties like PML-N had access to more extensive voter data, enabling features like automated calls and more accurate digital voter tools. Due to resource constraints, AWP focused on hard copies of voter lists rather than digital platforms.

JI similarly collected voter data manually through its grassroots campaigns, as they could not afford to retrieve digital data in bulk. The JI candidate mentioned that they did explore options like robocalls and mass messaging, however, they ultimately relied on manual WhatsApp and text messaging to connect with voters. Their campaign largely involved physical voter slips and community-based outreach efforts, supported by extensive volunteer work within local neighbourhoods.

PTI, despite facing restrictions on public gatherings, leveraged digital tools effectively. They accessed constituency-specific voter data from the ECP, including phone numbers, which they used for door-to-door campaigns and to send voice messages to voters. The PTI candidate also stated that they had a centralised data collection system, which they shared with candidates on CDs, allowing extensive voter outreach. Additionally, they used an election management app provided by the ECP for reporting polling data, which was particularly useful in overcoming technical issues like power outages or internet failures.

HKP also obtained voter lists from the ECP, though they encountered discrepancies, such as deceased voters remaining on the lists. Despite these challenges, they used the data to strategically focus on areas with larger voter populations. Their campaign included door-to-door outreach and boosted Facebook videos, with WhatsApp groups playing a significant role in maintaining communication with voters. As a smaller party, HKP relied heavily on volunteers and activists from across Pakistan to help spread their message both online and through pamphlet distribution in targeted areas.

Overall, the elections saw a blend of traditional and digital campaigning methods, with different levels of sophistication based on the resources and infrastructure available to each party.

10. Understanding of and willingness to incorporate transparency protocols

Political candidates showed varied perspectives on the importance and incorporation of transparency protocols in campaign spending, with concerns focused on the uneven application of rules, lack of oversight, and the role of external influences.

The PPP candidate acknowledged the importance of transparency in targeted election campaigns, emphasising that voters were increasingly aware of why they receive certain advertisements. However, she stressed the need for greater transparency in how political ads are targeted and

the involvement of civil society and lawmakers in initiating dialogue to address this issue. She also called for stakeholder collaboration to push transparency forward.

The AWP candidate expressed concerns about the legal spending limits for campaigns, stating that larger parties often exceeded the limits by collecting donations from supporters instead of funding everything on their own. This created significant loopholes in transparency, especially for online advertisements, and disproportionately disadvantaged smaller parties. He also highlighted the high cost of acquiring voter lists, which imposed additional financial burdens on candidates with limited resources.

The JI candidate emphasised that they aim to strictly adhere to rules set by the ECP. However, they criticised the broader system, echoing the narrative of other political candidates, pointing out that wealthy candidates were often able to bypass the rules and dominate elections through massive spending, including in digital marketing. The JI candidate also called for stricter enforcement of regulations to level the playing field and allow candidates with fewer resources to compete fairly.

The PTI candidate acknowledged the importance of transparency within their own party, praising its internal systems as transparent and well-organised. However, the interviewee critiqued external institutions, including the ECP, for disrupting transparency in the electoral process. He suggested that unless these external factors were controlled, transparency measures within individual parties would be ineffective in addressing the broader issues of dishonesty and manipulation.

The HKP candidate spoke in favour of stricter enforcement of transparency regulations, stating that unchecked spending by mainstream parties manipulates the election process. The candidate pointed out that smaller or independent candidates are more heavily scrutinised for minor violations, while larger parties are often given a pass. He also advocated for reduced campaign expenses to make elections, and entering politics more accessible to ordinary people, thus encouraging broader participation in the democratic process.

Overall, while parties across the spectrum acknowledged the importance of transparency, their ability and willingness to implement these protocols were often hindered by external pressures, financial constraints, and the uneven enforcement of regulations.

11. Voter Recommendations on Data Privacy

When voters were asked about how to improve data privacy, particularly concerning voter data, their responses revealed a range of concerns and recommendations. One voter highlighted the need for specific laws to protect data, especially considering how women are disproportionately

affected by privacy breaches. They explained how harassment and blackmail targeting women can escalate if personal information, such as phone numbers linked to CNICs, falls into the wrong hands. This can have long-lasting social consequences, particularly in conservative areas where a data breach might lead to women being forced into marriages or withdrawn from education.

Another voter stressed the importance of either granting all political parties equal access to voter data or preventing any party from using it at all. This comment stemmed from the perception that certain parties, such as PMLN, disproportionately used voter data in their campaigns, which created an imbalance in how political outreach was conducted.

There was also widespread mistrust toward the government and its institutions. Some voters mentioned the recent data breaches at NADRA and felt that their personal data was not adequately protected. One interviewee recommended that the government and telecommunications companies should handle citizens' data more responsibly and ensure that it is not used for political advertisements. This sentiment extended beyond elections, with one voter mentioning that even institutions like the Federal Board of Revenue (FBR) misuse personal data, creating an atmosphere of fear and mistrust.

Another key recommendation was the strengthening of institutions responsible for data privacy and security. Several voters believed that weak institutions were a major reason for the rampant misuse of personal data. One suggested that political parties should not have access to private data at all and instead focus on campaign messaging based on performance. The misuse of data, they argued, only exacerbates security issues.

Some voters also felt that data privacy policies should be simplified and made more accessible to the general public. One voter emphasised the importance of transparency and suggested that the government should make it easier for people to understand how their data is being used. Building public trust, they argued, is essential to addressing data privacy concerns.

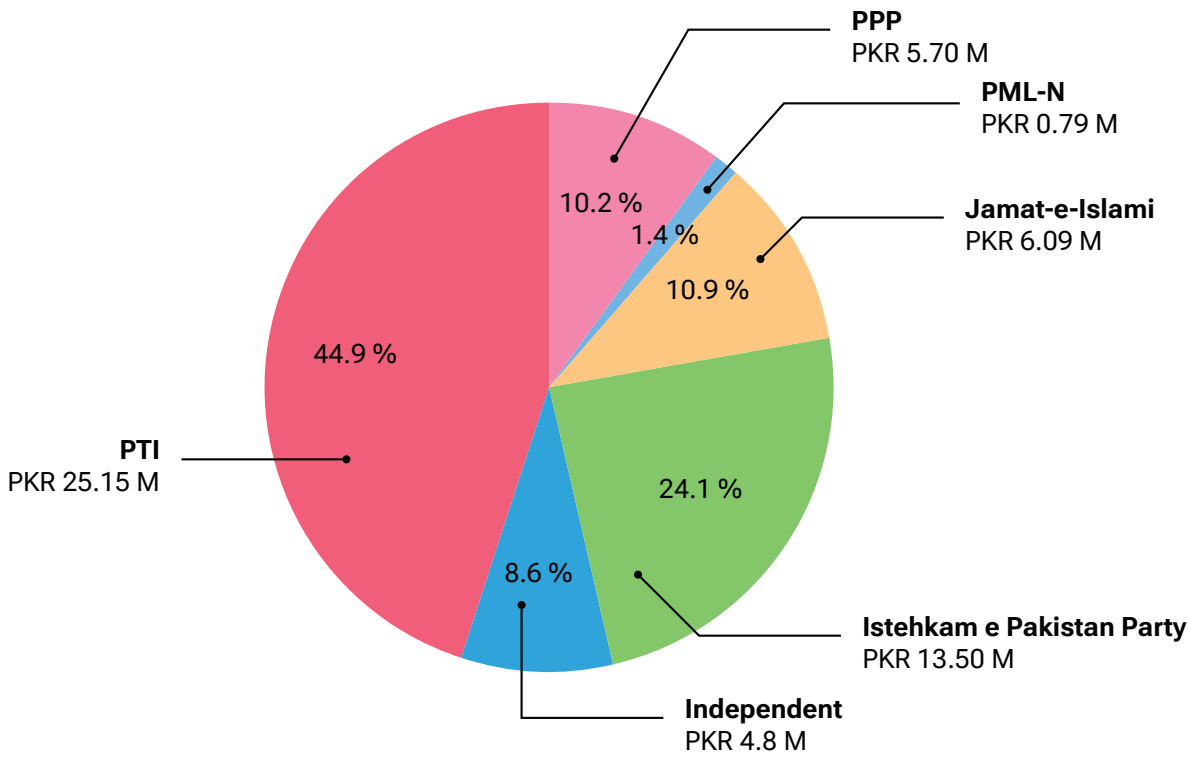
Finally, one voter recommended raising public awareness about data privacy rights. By educating citizens about the risks of data breaches and their rights under the law, they believed that people could be empowered to better protect their own personal information.

These recommendations reflect the concerns voters have about the lack of transparency and security regarding their personal data and highlight the urgent need for reforms to address the evolving challenges posed by data privacy in Pakistan.

POLITICAL ADVERTISEMENTS

Several political party candidates mentioned the use of political advertisements on social media to boost their election campaigns.

Party Spending on Political Advertisements (PKR Millions)



Digital Rights Foundation (2024) recently conducted research on platform accountability during elections, where we collected data on political advertisements from Metas ad library. Insights from that report show that PTI was the largest spender, accounting for 45.5% of the total spending. This totaled to around PKR 25.15 Million. This reflects the party's approach to campaign that relied mainly on social media to to state regulations determining the capacity at which the party could be involved in the elections. Social media seemed to be the only way for them to reach a broad audience across Pakistan.

PPP also had significant spending, indicating their active engagement in digital advertising to influence voter perceptions. PPP spent approximately 10.3% of the total spending. JI and independent candidates had smaller shares, suggesting limited resources as well as a more targeted campaign approach focusing on specific voter segments. Sitting at 1.4% share of political ads on Meta, PML-N did not partake much in online advertisements, as evidenced in

Meta's ad library report. However, there are reports of PML-N candidates independently paying for their election campaigns, although even those efforts were not significant enough compared to financial investments in online campaigns by PTI and PPP.

According to Section 182 of the Election Act 2017, all campaigning should cease 48 hours before election day (DAWN News, 2024). However, political ads continued to run and receive impressions on social media platforms during the restricted period of 6th Feb 2024 - 8th of feb 2024. This breach of election law by several parties reflects the challenges of enforcing traditional regulations in the digital landscape. Platforms failed to enforce local rules strictly, leading to an amplification of political content when it should have been halted (Digital Rights Foundation, 2024).

CONCLUSION

The digitization of politics has transformed how voter data is collected, used, and often misused, with significant implications for privacy and democratic integrity. Political parties now have access to vast amounts of personal information, some of which they acquire through legal means, while unethical means also tend to be employed. Citizen data is used for voter targeting, fundraising, and manufacturing ideologically driven communications. Micro-targeted messaging, designed to appeal to specific voter segments, raises concerns about informed consent and the ethical use of data, especially when it comes to organising free and fair elections.

While digitization offers smoother electoral processes, it has also opened the door to exploitation. Reports of political parties accessing unauthorised voter data and misusing digital platforms highlight the inadequacies in the existing regulatory framework. Low digital literacy further compounds the issue, as citizens often unknowingly share sensitive data, leaving them vulnerable to misuse. Without stronger data privacy protections, particularly for the most vulnerable populations, the risks of exploitation persist.

The future of electoral integrity hinges on the effective implementation of legislative measures that safeguard voter privacy, particularly as data-driven political campaigns become more prevalent. Strengthening regulatory frameworks is essential to protect personal information during elections and restore public trust in the electoral system.

RECOMMENDATIONS

1. Audit and Monitoring systems:

In order to enhance voter data privacy and to effectively safeguard citizens' personal data, a robust system of institutional audits and monitoring needs to be implemented. ECP and NADRA should go through regular checks to ensure that all systems are up to date and security measures are being followed. These audits should be carried out by independent third-party cybersecurity experts to ensure that no personal biases influence the process. Additionally, these audits should assess the vulnerabilities in the systems used for voter data collection, sharing, and storage - especially in light of recent data breaches and unauthorised access to sensitive files.

Similarly, rigorous audits of any election technology procurement process should also be put in place. Transparency during procurement, especially when it comes to handling voter data, prevents conflicts of interest and guarantees quality. The government's past experience with the Results Transmission System (RTS) further emphasises how crucial it is that new tech is tested beforehand and meets strict security and performance criteria.

2. Strict Data Sharing Regulations and Synchronisation:

Data sharing between NADRA, ECP, and political parties must be subject to strict protocols and regulatory frameworks. Only essential data should be shared, under clear, legally defined boundaries stipulating its use. Parties that receive voter data in the form of voter lists should be legally required to adhere to privacy and security protocols. NADRA and ECP should work on creating a synchronised database, reducing the time and resources needed to transfer data in between each other. This would also aid in limiting errors and discrepancies that occur during the process. However, even though synchronisation is important and will drastically improve the way voter data is managed, it is important to ensure that necessary protocols are in place to ensure that data is protected during said synchronisation processes, which is when data is vulnerable to external threats. Additionally, heightened safeguards should be incorporated for biometric and sensitive data, especially if it is susceptible to breaches. Since biometric data requires unique identifiers, it is essential that encryption standards are implemented. Additional protections such as limited personnel access and two factor authentication for database access would further improve security.

3. Collaboration for Improved Legislation:

NADRA and ECP should collaborate with experts and civil society organisations working on the issues to improve existing legislations such as the Elections Act and Election Rules 2017, which often fall short when it comes to effectively protecting voter data. Similarly, the Data protection Bill 2023 has not yet been passed, even after three updated drafts being proposed over the last few years. Getting that bill passed should be prioritised after meticulous revisions to address loopholes and evolving data privacy concerns.

4. Data security training:

Extensive training workshops must be organised and be made compulsory for personnel handling sensitive citizen data in institutions such as NADRA and ECP. These training sessions should focus on data security protocols, and the best practices for safeguarding sensitive citizen data. This would ensure that all personnel are aware of the ethical and legal consequences of data breaches. The training should emphasise the importance of adherence to strict protocols and tools, in compliance with data protection laws. Refresher courses should be held to address evolving technology updates as well as threats. Making these trainings mandatory will promote accountability and transparency - significantly reducing the likelihood of breaches.

5. Transparent Data Requests:

Political parties should be legally required to publicly disclose the amount of voter data they acquire through ECP. This would make the campaigning process more transparent, ensuring that parties adhere to data protection regulations, and prevent misuse. Public disclosure would also allow oversight bodies to monitor the data handling practices of political parties, ensuring that there is a level playing field and no party has an advantage over the other when it comes to accessibility to voter data. This would also require that the voter data not be sold on the basis of the number of voters, instead a fixed nominal fee could be charged so that all parties have equal access to data.

6. Public Autonomy:

Voters and citizens should be given more agency and autonomy to decide how their personal data is used by public officials, organisations, and political parties. At the point of collection, explicit consent should be retrieved from voters. It should be ensured that before written consent is taken from citizens, they fully understand how their data will be managed, and what options they have with regards to retracting their consent. Every time their information is shared by NADRA or ECP with a third party, they should be notified and should have the right to withdraw consent from their data being used.

7. Ethical Data Usage Policies in Political Campaigning:

Political parties must adopt and enforce stringent ethical data usage policies when managing vast amounts of voter data during campaigns. Parties must commit to only using data for legitimate campaign purposes, such as voter outreach, without engaging in manipulation or undue micro-targeting. All data collection efforts should comply with data protection laws, and any misuse of voter data should carry significant penalties.

8. Internal Political Party Data Audits:

Political parties should conduct regular internal audits of their data management systems to ensure compliance with data privacy laws and ethical standards. These audits should evaluate how voter data is collected, stored, processed, and shared within the party, with a focus on

identifying potential security vulnerabilities and areas where data may be misused. The audit process should involve independent experts to provide objective oversight and ensure transparency. Furthermore, audit reports should be made publicly available, demonstrating accountability and adherence to legal and ethical guidelines

9. Implementation of Election Rules and Regulations:

Strict implementation of election rules and regulations is necessary to ensure ethical campaign practices and uphold electoral integrity. Political parties must adhere to guidelines that promote fair competition and prohibit negative campaigning, hate speech, and the misuse of public resources. The Election Commission of Pakistan (ECP) should play a proactive role in monitoring campaigns, enforcing penalties for violations, and ensuring transparency in how political parties communicate with voters. Clear rules should be established regarding the use of digital platforms and voter data, preventing manipulative tactics like micro-targeting without consent. Regular audits of campaign conduct, coupled with public reporting of any violations, will help maintain decorum and respect for voter privacy during the election process.

10. Transparency & accountability in voter targeting by telecommunication companies:

Telecommunication companies must be held accountable for how they handle and share voter data, especially when it comes to targeting individuals for political campaigns. To ensure transparency, these companies should be required to publicly disclose any agreements or data-sharing arrangements with political parties or government institutions. Clear guidelines should be established to prohibit the unauthorised use of personal information for voter targeting. Additionally, telecom companies should be subject to independent audits to verify compliance with data privacy laws, and any misuse of data should result in stringent penalties. Enforcing these measures would help restore public trust and prevent the unethical exploitation of citizen data for political gain.

11. Transparency and Oversight on Social Media Spending:

Political parties should be required to maintain full transparency and accountability when allocating significant funds to social media platforms for campaign purposes. Clear regulations should mandate that political parties report these expenditures to the Election Commission of Pakistan (ECP), which in turn should regularly audit these expenditures to ensure compliance with legal and ethical standards. Additionally, political ads should be clearly labelled, and parties should be held responsible for ensuring that their ads do not spread misinformation or target voters in ways that violate privacy laws.

REFERENCES

Abbas, Z. (2024, July 2). *The surveillance system keeping tabs on millions - Pakistan - DAWN.COM.* Dawn. https://www.dawn.com/news/1843299

Abbasi, S., & DAWN. (2019, June 2). *HOW VULNERABLE IS YOUR PERSONAL DATA? - Newspaper - DAWN.COM.* Dawn. https://www.dawn.com/news/1485925/how-vulnerable-is-your-personal-data

Abbasi, S., & DAWN Prism. (2024, October 22). *Caught in the web: Surveillance, data protection and AI in Pakistan.* DAWN Prism. https://www.dawn.com/news/1864073

Baloch, M., & Musyani, Z. (2020, July 8). *Pakistan's Great Digital Divide – The Diplomat.* The Diplomat. https://thediplomat.com/2020/07/pakistans-great-digital-divide/

Boldyreva, E. (2018, December). *Cambridge Analytica: Ethics And Online Manipulation With Decision-Making Process.* ResearchGate. https://www.researchgate.net/publication/330032180_Cambridge_Analytica_Ethics_And_Online_Manipulation_With_Decision-Making_Process

Community of Democracies. (2022, June). *Technology in Elections – Best Practices in Using Digital Tools and Platforms in the Community of Democracies.* Community of Democracies. https://community-democracies.org/app/uploads/2022/09/Report-Technology-in-Elections.pdf

Dad, N., & Khan, S. (2023). Reconstructing elections in a digital world. South African Journal of International Affairs, 30(3), 473–496. https://doi.org/10.1080/10220461.2023.2265886

Data Protection Act, No. 9 of 2022. (2022). *Sri Lanka: Personal Data Protection Act No. 9 of 2022.*https://www.dataguidance.com/sites/default/files/personal_data_protection_act_no._6_of_2022.pdf

DAWN. (2018, June 20). *No breach of voters' data security: Nadra - Newspaper - DAWN.COM.* Dawn. https://www.dawn.com/news/1414889

DAWN News. (2024, January 9). *Article published in The Economist authored by Imran, not compiled using AI: PTI.* Dawn. https://www.dawn.com/news/1804477

DAWN News. (2024, February 6). *Last steps to polls as campaigns end tonight.* https://www.dawn.com/news/1811534

DAWN News & Nasir, A. (2023, April 7). *PAC orders inquiry into breach of army chief, family's personal data.* Dawn. https://www.dawn.com/news/1746352

Dawn. (2023, October 31). I*ndia's data protection law draws scrutiny at global meet.* Dawn. https://www.dawn.com/news/1784472

Digital Rights Foundation. (2024, December). *Platforms at the Polls: Disinformation, Political Ads & Accountability during the 2024 Pakistan General Elections.* Digital Rights Foundation. https://digitalrightsfoundation.pk/wp-content/uploads/2024/12/Platforms-at-the-Polls.pdf

Digital Rights Monitor & Shahid, U. (2023, December 4). *Illicit website offering mobile subscription, CNIC data found advertised on news platform.* Digital Rights Monitor. https://digitalrightsmonitor.pk/illicit-website-offering-mobile-subscription-cnic-data-found-advertised-on-news-platform/

DLA Piper. (n.d.). *Data protection laws of the world: Pakistan and Sri Lanka.* DLA Piper Data Protection Handbook. https://www.dlapiperdataprotection.com/index.html?t=law&c=PK&c2=LK

Dobber, T., Fathaigh, R. Ó., & Borgesius, F. J. Z. (2019, December 31). *The regulation of online political micro-targeting in Europe.* Internet Policy Review. https://policyreview.info/articles/analysis/regulation-online-political-micro-targeting-europe

Durrani, Z. (2024, February 8). *Data Privacy: Elections And Beyond.* The Friday Times. https://thefridaytimes.com/08-Feb-2024/data-privacy-elections-and-beyond

EFE. (2024, March 27). *The Pakistan Data Leak Scandal: 2.7 Million Citizens Affected - EFE Noticias.* Agencia EFE. https://efe.com/en/economy/2024-03-27/personal-data-of-2-7-million-pakistanis-stolen-from-government-records-probe-find/

European Commission. (2021, March). *Study on the impact of new technologies on free and fair elections ('Elections Study') Literature Review.* European Commission. https://commission.europa.eu/system/files/2022-12/Annex%20I_LiteratureReview_20210319_clean_dsj_v3.0_a.pdf

The Express Tribune. (2018, June 30). *Voters data leakage claim: NADRA issues legal notice to ex-deputy chairman.* https://tribune.com.pk/story/1746598/voters-data-leak-nadra-frames-former-official-theft

The Guardian. (2023, December 18). *Imran Khan deploys AI clone to campaign from behind bars in Pakistan.* The Guardian. https://www.theguardian.com/world/2023/dec/18/imran-khan-deploys-ai-clone-to-campaign-from-behind-bars-in-pakistan

Hanna, T. (2024, July). *What Is Data Privacy? | Definition from TechTarget.* TechTarget. https://www.techtarget.com/searchcio/definition/data-privacy-information-privacy

Judge, E. F., & Pal, M. (2021). Voter Privacy and Big-Data Elections. *Osgoode Hall Law Journal, 58(1).* https://digitalcommons.osgoode.yorku.ca/ohlj/vol58/iss1/1

Kamran, H., Khan, S., Rana, S., Rehman, Z., Malik, M., & Media Matters for Democracy. (2022, May). *Connecting the Disconnected: Mapping Gaps in Digital Access in Pakistan.* https://mediamatters.pk/wp-content/uploads/2022/06/Connecting-the-Disconnected-Report.pdf

Kapoor, N., & Mukherjee, P. (2023, October 11). *Understanding India's new data protection law.* Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2023/10/understanding-indias-new-data-protection-law?lang=en

Karjian, R. (2018). *What is Data Protection and Why is it Important? A Guide.* TechTarget. https://www.techtarget.com/searchdatabackup/definition/data-protection

Khan, M., Ahmed, T., & Hussain, F. (2022). *Survey on technological penetration across provinces in Pakistan.* Springer. https://link.springer.com/article/10.1007/s10708-022-10781-7

Khan, M. A., & Sheikh, A. A. (2022). *Privacy, data protection, and cyber crimes: Mapping perceptions and experiences in digital landscapes.* Typeset. https://typeset.io/papers/privacy-data-protection-and-cyber-crimes-mapping-perceptions-2ymi2tgh8p

Klosowski, T. (2024, April 16). *How Political Campaigns Use Your Data to Target You.* Electronic Frontier Foundation. https://www.eff.org/deeplinks/2024/04/how-political-campaigns-use-your-data-target-you

Koehnke, F. (2022). *An introduction to the Digital Personal Data Protection Bill of India.* German National Library. https://d-nb.info/1262674220/34

Manyika, J., Chui, M., Brown, B., Bughin, J., Dobbs, R., Roxburgh, C., & Byers, A. H. (2011, May). Big data: The next frontier for innovation, competition, and productivity. *McKinsey Digital.* https://www.mckinsey.com/capabilities/mckinsey-digital/%20our-insights/big-data-the-next-frontier-for-innovation

The Nation. (2024, March 28). *Eight NADRA officials suspended as action 'begins' in data theft case.* The Nation. https://www.nation.com.pk/28-Mar-2024/eight-nadra-officials-suspended-as-action-begins-in-data-theft-case

Nurse, J. R., Agrafiotis, I., Erola, A., Bada, M., Roberts, T., Williams, M., Goldsmith, M., & Creese, S. (2017, May 13). An Assessment of the Security and Transparency Procedural Components of the Estonian Internet Voting System. *Human Aspect of Information Security, Privacy and Trust, 366-383.* https://doi.org/10.1007/978-3-319-58460-7_26

Personal Data Protection Act, 2010. (2010). *Malaysia: Personal Data Protection Act 2010.* https://www.pdp.gov.my/jpdpv2/assets/2019/09/Personal-Data-Protection-Act-2010.pdf

Privacy International. (2019, June). *Technology, data and elections: A 'checklist' on the election cycle.* Privacy International. https://privacyinternational.org/sites/default/files/2019-07/Technology%2C%20data%2C%20and%20elections_0.pdf

PrivacyWorld. (2024, August). *Malaysia pushes out ground breaking amendment to the Personal Data Protection Act: Impact on businesses.* PrivacyWorld Blog. https://www.privacyworld.blog/2024/08/malaysia-pushes-out-groundbreaking-amendment-to-personal-data-protection-act-impact-on-businesses

PRS Legislative Research. (2023, August 9). *Digital Personal Data Protection Bill, 2023.* PRS Legislative Research. https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023

Qarar, S., & DAWN News. (2017, June 9). *Nadra responds to Wikileaks, denies ever sharing data with foreign countries.* Dawn. https://www.dawn.com/news/1338486

Raza, S. I., & DAWN News. (2012, July 24). *Nadra conducts its own probe into 'UK visa scam'.* DAWN. https://www.dawn.com/news/736956/nadra-conducts-its-own-probe-into-uk-visa-scam

Shah, N., Malik, A., & Baig, Z. (2023). *Understanding the disparity in technological infrastructure and survey participation across Pakistan.* Springer. https://link.springer.com/article/10.1007/s11205-023-03300-9

Shahid, M., Rauf, M., Gulzar, A., & Faiz, R. (2022). *Students of higher education institutions (HEIs) and information and communication technologies (ICTs): Viability of digital media literacy in Pakistan.* ResearchGate. https://www.researchgate.net/publication/360779580_Students_of_Higher_Education_Institutions_HEIs_and_Information_and_Communication_Technologies_ICTs_Viability_of_Digital_Media_Literacy_in_Pakistan

Shree. (2023, May 5). *When parties toy with voters' privacy.* Deccan Herald. https://www.deccanherald.com/india/karnataka/bengaluru/when-parties-toy-with-voters-privacy-1216175.html

Silva, S. d., & EngageMedia. (2022, June). *Through the Looking Glass: Digital Safety and Internet Freedom in South and Southeast Asia.* Engage Media. https://engagemedia.org/wp-content/uploads/2022/06/EngageMedia_Report-GIF-Report_06082022.pdf

United Nations Development Programme (UNDP). (2024, April). Doing Digital for Development. https://undppknhdr2024.com/wp-content/uploads/2024/09/NATIONAL-HUMAN-DEVELOPMENT-REPORT-2024.pdf

World Tomorrow by Wikileaks (Writer). (2012, June 19). (Episode 10) [TV series episode]. In *The Julian Assange Show.* https://youtu.be/rw4KxdUMiL0?si=LlKm9J6YSq8_2h6F

Younus, U. (2024, February 14). *Five ways Imran Khan's party used technology to outperform in Pakistan's elections.* Atlantic Council. https://www.atlanticcouncil.org/blogs/new-atlanticist/five-ways-imran-khans-party-used-technology-to-outperform-in-pakistans-elections/

DigitalRightsFoundation
"KNOW YOUR RIGHTS"

@digitalrightsfoundation

@DigitalRightsFoundation

@DigitalRightsPK

@digitalrightsfoundation

@digitalrightsfoundation

@DigitalRightsPK