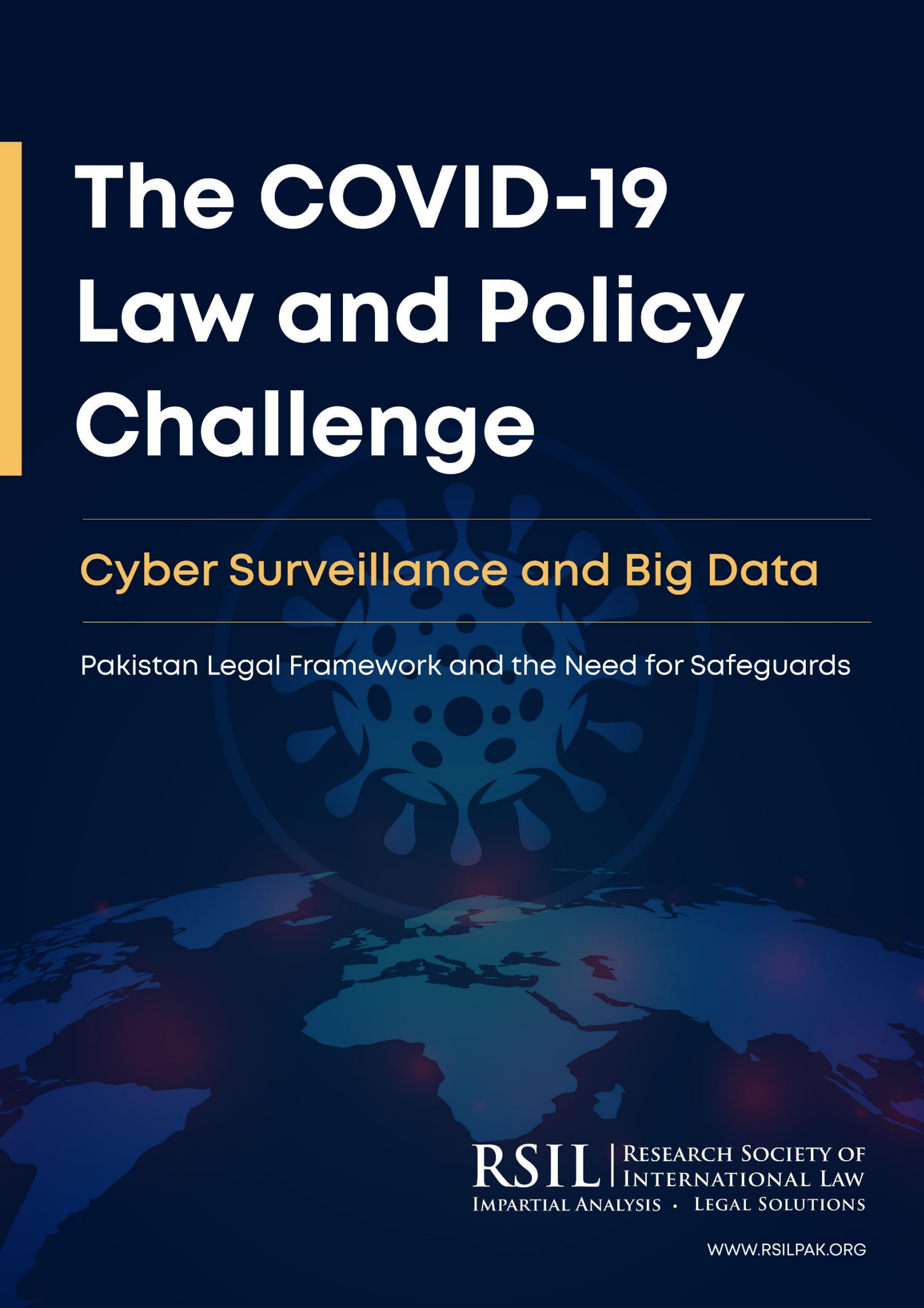
The COVID-19 Law and Policy Challenge

Cyber Surveillance and Big Data

Pakistan Legal Framework and the Need for Safeguards



RSIL | Research Society of International Law
Impartial Analysis • Legal Solutions

WWW.RSILPAK.ORG

The COVID-19 Law & Policy Challenge

Cyber Surveillance and Big Data: Pakistan's Legal Framework and the Need for Safeguards

Authors:

Oves Anwar
Director Research, RSIL

Ayesha Malik
Senior Research Associate, RSIL

Abraze Aqil
Research Associate, RSIL

Noor Fatima
Research Associate, RSIL

RSIL | RESEARCH SOCIETY OF INTERNATIONAL LAW
IMPARTIAL ANALYSIS • LEGAL SOLUTIONS

TABLE OF CONTENTS

1. Introduction

The on-going effort to curb the spread of COVID-19 has led to the adoption of various technologies in order to achieve public health outcomes. The proliferation of cyber surveillance to monitor and map the outbreak brings with it a range of challenges and opportunities. This paper highlights potential legal issues caused by the use of such measures, by analysing both the existing legal framework in Pakistan and model legislation. This covers laws that enable the adoption of such technologies, laws which protect privacy, and recommendations to appropriately balance the need to act in the interest of public health with human rights, specifically individual privacy.

2. Overview of Cyber Surveillance Issues – Health v. Privacy

As discussed in detail in Paper 1 of this series, heightened surveillance under emergency laws run the risk of being misused and individuals' right to privacy violated. It is imperative to balance the level of interference with the right of privacy and ensure overall adherence for human rights while countering the pandemic. International law, through the International Covenant on the Civil and Political Rights (ICCPR) and the Siracusa Principles of 1985 offer guidance as to how this balance may be struck. The legitimate aim (i.e. public health) can limit enjoyment of a right so long as it is done by law and when necessary and proportionate to such aims. As a result, an 'infected unless proven healthy' approach has been advocated which would allow individuals to voluntarily download an application which would gather their data, this data would be anonymised and aggregated so that personal identifiers are not used, and strictly limited in time. This would enable the State to effectively utilise citizens' data to stem the rate of infection while protecting their data and privacy by avoiding draconian measures. This paper will chart the State's ability to do so through its legal framework, and conclude with recommendations to bolster the same.

3. Pakistan's Legal Framework

a) The Right to Privacy

The Constitution

The right to privacy is enshrined as a fundamental right in Pakistan's Constitution under Article 14(1), which states that "[t]he dignity of man and, subject to law, the privacy of home, shall be inviolable."[1] Whilst this provision only refers to the privacy of the home, in order to provide meaningful protection of the right to privacy, the Superior Courts have read it in an expansive manner to include a general right to privacy everywhere.[2]

A complementary right to privacy, is the right to information which is found in Article 19A: "Every citizen shall have the right to have access to information in all matters of public importance subject to regulation and reasonable restrictions imposed by law." This is important in the discussion regarding cyber surveillance because of the sheer volume of data (including private or otherwise sensitive information) collected by state authorities, and thereby empowers citizens to have access to that information under this context.

[1] The Constitution of the Islamic Republic of Pakistan – National Assembly

[2] Ghulam Hussain v. Additional Sessions Judge, Dera Allah Yar, PLD 2010 Quetta 21; Mushtaq Ahmed and Others v. Secretary; Ministry of Defence through Chief of Air and Army Staff; PLD 2007 Kar.; Muhammad Abbas Alias Ajmi v. State, 2005 YLR 3193; Benazir Bhutto v. President of Pakistan, PLD 1998 SC 388; Chamber of Commerce and Industry v. Director General Quetta Development Authority, PLD 2012 Bal 31; Ghulam Hussain v. Additional Sessions Judge, Dera Allah Yar, 2010 PLD 21 Quetta High Court Balochistan; Master Bilawal Ali Zardari v. K.D.A, PLD 1993 Kar 67; M.D Tahir v. State Bank, 2004 CLC 1680 Lahore

Federal Laws

Currently, at the federal level, there is no overarching statute that governs cyber surveillance, data collection or the data rights of citizens in Pakistan.

At the time of writing, the **Personal Data Protection Bill 2020** is under consultation from relevant public and private sector stakeholders, but has not as yet been enacted by Parliament. Prior to this, the **Personal Data Protection Bill of 2018** was proposed by the Ministry of Information Technology and Communications (MOITT). The Bill sought to outline the responsibilities of data collectors and processors as well as rights and privileges of consumers while criminalizing misuse of data. However, this was never presented to the Parliament and is now replaced with the 2020 Bill.

Apart from these, the **Freedom of Information Ordinance (2002)** offers some guidance on issues of privacy. As per Section 17 of the Ordinance, the disclosure of certain forms of information is exempt if its disclosure would invade the privacy of an identifiable individual other than the requester.

The proposed **Personal Data Protection Bill 2020** in Pakistan attempts to structure, and furnish digital rights of citizens, amongst other frameworks to ensure data privacy.[3]

A welcome addition has been the inclusion of 'consent' in the proposed legislation. Section 2(l) defines consent as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the collecting, obtaining and processing of personal data relating to him or her."[4] However, there is no clarity how consent can be given through "clear affirmative action," and neither is there any indication as to what this term precisely denotes. Similarly, there is a further need to explore in detail what "personal data", including 'sensitive personal data' refer to (Section 2(k)).[5]

The 2020 Bill recognizes digital rights such as the right to access data (S. 16), right to correct data (S. 19), withdrawal of consent to process data (S. 23-25), rights of foreign data subjects (S. 26), right to erasure of data (S. 27). Furthermore, while Sections 8 and 9 create provisions regarding data security and retention, no time limits are defined for these purposes.

As well, the exceptions are granted under Sections 31 to the federal government in situations, granting it the power to exempt, pose terms and conditions on or revoke any order made under this Act. In Section 38, the federal government is empowered to issue policy directives directly to the Authority, to which the latter will comply. However, both these sections are ambiguous and

[3] Personal Data Protection Bill 2020 (Consultative Draft) - Ministry of Information Technology and Telecommunications https://www.moitt.gov.pk/SiteImage/Downloads/Personal%20Data%20Protection%20Bill%202020%20Updated.pdf

[4] Section 2(l): Personal Data Protection Bill 2020 (Consultative Draft) - Ministry of Information Technology and Telecommunications

[5] Section 2(k): "sensitive personal data" means and includes data relating to access control (username and/or password), financial information such as bank account, credit card, debit card, or other payment instruments, and, passports, biometric data, and physical, psychological, and mental health conditions, medical records, and any detail pertaining to an individual's ethnicity, religious beliefs, or any other information for the purposes of this Act and rules made thereunder [Personal Data Protection Bill 2020]

broad, and may be used to shirk parliamentary scrutiny and accountability.[6] Furthermore, throughout the document, broader "public interest" is invoked in various sections, but the term has not been defined and there is thus a chance that it may be misconstrued or misused by authorities.

The Right to Privacy and the Courts

In Pakistan, case law pertaining to privacy remains scarce and most cases have little to do with digital or cyber-surveillance. However, while Article 14 of the Constitution refers to the privacy of the home, the definition and scope of the right has been extensively expanded upon and can now be said to include the right to privacy, as held in Taufiq Bajwa v. CDGK, allowing a person freedom from public scrutiny, provided that the individual does not act in an unlawful manner.[7] The courts have held that since any intrusion into the privacy of a person necessarily violates the privacy of home, and by extension injures the dignity of man, it may only be taken away by the State for extraordinary reasons, such as in cases of national security.[8] The privacy of the home is specifically recognized as a fundamental right and this extends to people who enter public spaces where they are entitled to limited personal space and privacy.[9]

It has also been held that the right to privacy is violated where private correspondences are read,[10] or where non-physical intrusions such as spying occur.[11] In M.D. Tahir v. State Bank, the Lahore High Court held that the practice of collecting the private information of bank holders and presenting them to tax authorities, without any allegation of wrongdoing was a violation of the right to privacy.[12] The State Bank of Pakistan had previously issued a directive that called for the collection, without any sustainable juridical criteria, of personal information like name, address, NTN Number and NIC Numbers of individuals who have obtained ten thousand rupees as interest. The directive was struck down and it was held that "taking of private information without any allegation of wrongdoing of ordinary people is an extraordinary invasion of this fundamental right of privacy."

In Taufiq Bajwa vs CDGK, the petitioner argued that his right to life under Article 9 of the Constitution had been violated by the boundary wall of a neighbouring park which was of such a height that it allowed a person to look inside his home.[13] The court supported the petition and held that the park and wall must be reconstructed such that the petitioner's privacy is not violated. The case affirms that the courts interpret Article 9 ("right to life") widely enough to be used to protect the right to privacy.

[6] Personal Data Protection Bill 2020 – Civil Society Submission to the Ministry of Information Technology and Telecommunications, May 2020, Digital Rights Forum.
[7] Taufiq Bajwa vs CDGK (2010 YLR 2165)
[8] Muhammad Abbas Alias Ajmi v. State, 2005 YLR 3193; Benazir Bhutto v. President of Pakistan, PLD 1998 SC 388
[9] Chamber of Commerce and Industry v. Director General Quetta Development Authority, PLD 2012 Bal 31
[10] Ghulam Hussain v. Additional Sessions Judge, Dera Allah Yar, 2010 PLD 21 Quetta High Court Balochistan
[11] Master Bilawal Ali Zardari v. K.D.A, PLD 1993 Kar 67
[12] M.D.Tahir v. State Bank (2004 CLC 1680)
[13] Taufiq Bajwa vs CDGK (2010 YLR 2165)

b) Laws Specific to Infectious Diseases and Epidemics

Federal Laws

The only law which applies specifically to diseases in Pakistan is the outdated **Epidemic Diseases Act 1897** which was passed to deal with the bubonic plague epidemic in Bombay (now Mumbai).[14] It empowers officials to enter into any house and forcibly examine a suspected sick person, however, it does not authorize the government to enforce a lockdown, screen passengers, or institute any kind of surveillance. The law was amended in 1958 and renamed as the West Pakistan Epidemic Diseases Act, 1958 but the only amendments in the text were to replace the word India with Pakistan.

Provincial Laws

As health is a devolved subject after the 18th Constitutional Amendment, the onus of ensuring adequate healthcare in the event of a pandemic falls to the provinces. Whether these local laws include provisions allowing for surveillance will be analysed in this section.

The Punjab government recently passed the **Punjab Infectious Diseases Prevention and Control Ordinance (2020)**. The ordinance does not include any provisions relating to the role of cyber surveillance mechanisms and only indirectly alludes to data privacy in Section 27, where it states that any information regarding an infected person will be kept confidential and only released on consent, or to medical practitioners, etc.[15]

Sindh passed the **Sindh Epidemic Diseases Act 2014** which merely grants powers to the Government to take action to counter the spread and the impact of the disease.[16] There is no mention of collection of data of affected persons or confidentiality thereof.

In Balochistan, there is no dedicated ordinance or statute that defines the legal framework of action that can be undertaken to counter a communicable disease. With the COVID-19 outbreak, District Commissioners of all 33 regions were granted powers to impose penalties including imprisonment and fines to counter the coronavirus under Sections 3 and 4 of the **West Pakistan Epidemic Diseases Act 1958**.[17]

The **Khyber Pakhtunkhwa Public Health (Surveillance and Response) Act 2017** creates relevant authorities to counter diseases, defines their roles, and lays out the conditions required to announce public health emergencies in KP.[18] Section 8(b) of the Act states that the Provincial Disease Surveillance Center is responsible for ensuring that after verification, "all information and data with regard to events, diseases and persons affected with notified diseases or other diseases and conditions" be communicated to the public health committee for further assessment. With regards to the privacy and protection of this data, Section 13(2) states:

> "(2) In protection of public health, the Government shall ensure maintenance of secrecy of personal health information and data of the citizens in a manner that the same is not

[14] The Epidemic Diseases Act, 1958 - (W.P. Act XXXVI of 1958)
[15] The Punjab Infectious Diseases (Prevention and Control) Ordinance, 2020 (II OF 2020)
[16] The Sindh Epidemic Diseases Act, 2014 (No. VIII OF 2015)
[17] DCs Empowered to Fight the Coronavirus, Balochistan Express, March 2020
https://www.bexpress.com.pk/2020/03/dcs-empowered-to-fight-coronavirus/
[18] The Khyber Pakhtunkhwa Public Health (Surveillance and Response) Act, 2017 (No. XXX of 2017)

> disclosed to any person so as to cause any damage to the respect, dignity and reputation of the citizens."

However, no specific penalties are laid out in this Act in the instance of breach of privacy or data leaks.

The **Khyber Pakhtunkhwa Epidemic Control and Emergency Relief Ordinance 2020**[19], similar to the Punjab Ordinance 2020, only briefly alludes to the treatment of information collected on persons affected by COVID-19. Section 37 of the Ordinance states that information regarding an infected person will be kept confidential and only released on consent, or to medical practitioners, etc.[20]

Therefore, while provincial laws exist which would govern the local government's handling of the pandemic, with the exclusion of Khyber Pakhtunkhwa, they do not include provisions relating to surveillance or to the privacy of patient data. KP's law is a welcome step in that regard as it provides for the privacy and protection of patient data, however, the lack of penalties for a breach of privacy is problematic.

c) Laws on Cyber-Surveillance

In Pakistan, laws that pertain to or otherwise incorporate elements of cyber surveillance in its clauses usually do so from a criminal investigation perspective. Mass gathering of data for the purpose of disease or epidemic surveillance does not exist within the ambit of the current legislation, as illustrated below.

A number of laws do allow for agents of the state to engage in cyber-surveillance. Section 54(1) of the of the **Pakistan Telecommunications (Re-organisation) Act, 1996** provides that the "in the interest of national security or in the apprehension of any offense," the federal government may authorise any person to intercept calls or messages, or to trace calls made through any telecommunications system for national security reasons or for the investigation of any crime.[21] This allows the government to authorise surveillance. Section 57(2)(ah) authorises the Federal Government to make rules on the interception of communications without setting any standards. Under Section 8 of the Act the Federal Government may issue legally binding policy directives to the PTA in relation to certain telecommunications matters, including the requirements of national security.

This power, however, is not without limits, as set out by the Islamabad High Court:[22]

> "apprehensions relating to public safety, law and order or the happening of an untoward incident can by no stretch of the imagination attract Section 54(2) [of the Pakistan Telecommunications (Re-organization) Act, 1996] … and it can only be invoked if there is a Proclamation of Emergency by the President pursuant to powers vested under Part X of the Constitution…"

[19] Khyber Pakhtunkhwa Ordinance XI of 2020
[20] The Punjab Infectious Diseases (Prevention and Control) Ordinance, 2020 (II OF 2020)
[21] Pakistan Telecommunications Act 1996 (Act No. XVII of 1996)
[22] CM Pak Ltd. v. Pakistan Telecommunication Authority, 2019 (PLD 2018 Islamabad 243)

It is also of note that Article 260 of the Constitution of Pakistan, which defines the term 'Security of Pakistan'[23], does so while specifically excluding matters pertaining to "public safety", and therefore any reliance placed on national security provisions within the Pakistan Telecommunications (Re-organization) Act, 1996, as a means of surveilling the population at large, would seem to be contrary both to the ordinary constitutional construction, and to the Act itself. As individuals are entitled to be dealt with in accordance with the law[24]—especially when governmental action might be detrimental to the life, liberty, body, reputation, or property of any person—it is necessary that any actions taken, even in situations such as the present one where mass surveillance might serve an ostensible purpose, be done within the limits of applicable law.

The **Investigation for Fair Trial Act, 2013** allows for access to data, emails, telephone calls, and any form of computer or mobile phone-based communication, subject to a judicial warrant.[25] A warrant can be requested wherever an official has 'reasons to believe' that a citizen is, or is 'likely to be associated' with, or even 'in the process of beginning to plan' a terrorism or terrorism-related offence under Pakistani law. However, this would require the citizen to be specified, and in any case, the Act also allows for a judge to recommend departmental action against an officer if the judge is of the opinion that the warrant resulted in an undue and inappropriate interference of privacy, which necessarily limits the use of this Act as a tool for mass surveillance.[26]

Section 32 of the **Prevention of Electronic Crimes Act, 2016** requires telephone and Internet Service Providers to retain traffic data for at least one year.[27] Law enforcement bodies can demand access to that data subject to a warrant issued by a court. This may allow the government to access swathes of data for surveillance purposes. Section 30 allows courts to issue a warrant to a law enforcement officer to search and seize any data that "may reasonably be required" for a criminal investigation. However, Section 41 of the Act punishes unlawful disclosure of seized data with imprisonment of up to 3 years, and a fine of PKR 1 million.[28] Given that any disclosure in the context of the COVID-19 epidemic would fail to meet the standard of having been lawfully shared in the course of a criminal investigation, this does not provide for an avenue for mass surveillance.

Pakistan also has laws which impose regulations on social media and may be used to spread the curb of disinformation. The **Citizens Protection Rules (Against Online Harm) 2020** require social media companies to establish representative offices in Pakistan, to remove any 'unlawful content' within 24 hours, to prevent live streaming of any content "related to terrorism, extremism, hate speech, defamation, fake news, incitement to violence and national security."[29] If a company does not comply, its services can be blocked and it may face fines of up to 500 million rupees. This is important for the current COVID-19 crisis due to firstly, the proliferation of misinformation regarding the disease on social media platforms; and secondly, to potentially collate information gathered through such mediums for the detection of outbreak clusters.

The **National Disaster Management Authority Act, 2010** passed after the 2010 floods, aims to establish robust mechanisms to handle future disasters in a coordinated manner.[30] To that end, it calls for the establishment of a number of authorities and commissions to counter disasters. These authorities collectively have served as the focal point in governmental responses to the COVID-

[23] Article 260, Constitution of Pakistan, 1973: *"Security of Pakistan" includes the safety, welfare, stability and integrity of Pakistan and of each part of Pakistan, but shall not include public safety as such;*
[24] Article 4, Constitution of Pakistan, 1973
[25] Investigation of Fair Trial Act, 2013 (Act No. 1 of 2013)
[26] Section 15 of the Investigation of Fair Trial Act, 2013
[27] Prevention of Electronic Crimes Act, 2016 (Act No. XL of 2016)
[28] Section 41 of the Prevention of Electronic Crimes Act, 2016
[29] Citizens Protection Rules (Against Online Harm) 2020
[30] National Disaster Management Act, 2010 (Act No. XXIV of 2010)

19 epidemic, with District Authorities empowered to prevent and mitigate the effect of the pandemic in the form of directing local authorities[31], stockpiling[32] and distribution of relief goods and other resources[33], controlling movement of persons[34], as well as taking any additional steps that are warranted.[35]

Given the extraordinary nature of the powers granted by the Act and the extraordinary circumstances that are currently present, it is conceivable that cyber-surveillance may be allowed under the law, with measures potentially being imposed under the rubric that they are 'additional steps that are warranted' However, given the lack of specificity in the law, and the wide-ranging implications on fundamental freedoms caused by its operation, such actions would be subject to intense scrutiny in the Courts, and would be better served with action taken under laws tailor-made to covering cyber-surveillance in a pandemic scenario, wherein privacy protections and accountability procedures are baked in.

d) Big Data in Pakistan

The **National Database and Registration Authority Ordinance, 2000** establishing NADRA, Pakistan's database authority, states in Section 4(j) that it shall be responsible for ensuring "due security, secrecy and necessary safeguards for protection and confidentiality of data and information contained in or dealt with by the National Data warehouse at individual as well as collective level."[36] Therefore, NADRA is obligated to ensure that the data is anonymised or pseudonymised in order to protect the identities of citizens submitting information and bio-data as per legal requirements.

Section 4 of the **Monitoring and Reconciliation of Telephony Traffic Regulations, 2010** also requires network operators to establish a system that allows for real-time monitoring and recording of traffic on its networks.[37] Regulation 4(6) also requires that they enable the monitoring, measuring, controlling and recording of traffic in real-time, that they maintain a complete record of all communication signals (including for, but not limited to, billing purposes) and that they maintain a complete list of all Pakistani customers and their details.

The Punjab Safe City Authority (PCSA) established under the **Punjab Safe Cities Ordinance 2015** also invested heavily in big data/AI technologies to ensure the effective monitoring of citizens in the city of Lahore. In the Lahore Safe City Project, an integrated, city-wide communications and surveillance system brought together information from 15 Emergency Control and Despatch Control suites, 8000 CCTV cameras, specialized traffic monitoring systems, road side variable messaging systems and utilised 4G networks.[38] Some of the functions of these technologies included face recognition and vehicle tracking (with access to NADRA records), with the capacity to track individuals, record and transmit that data to be used by others for more than one purpose for an extended period of time. Although the PSCA has developed clear data protection policies and its Privacy Policy is publicly available, there have still been reports of leaked footage and misuse of images which breach individual privacy.[39]

---

[31] Section 20(2)(e) of the National Disaster Management Authority Act, 2010
[32] Section 20(2)(p) of the National Disaster Management Authority Act, 2010
[33] Section 22(a) of the National Disaster Management Authority Act, 2010
[34] Section 22(c) of the National Disaster Management Authority Act, 2010
[35] Section 22(m) of the National Disaster Management Authority Act, 2010
[36] National Database and Registration Authority Ordinance, 2000 (Ordinance VIII of 2000)
[37] Monitoring and Reconciliation of Telephony Traffic Regulations, 2010 (SRO 186(I)/2010)
[38] Advanced digital and security technologies help promote a safer Lahore – Lahore Safe City Project, ARUP Consultants https://www.arup.com/projects/the-lahore-safe-city-project
[39] Aiza Tariq, Privacy breach fears loom over Punjab Safe City Project, Pakistan Today, August 2018

e) Global Best Practices: GDPR (EU) and CCPA (US)

Why do we need data protection laws?

The 21st century is defined by advancements in information technology, which generates copious amounts of data on private individuals. The increased sophistication and multiplicity of uses of said data presents a number of unprecedented challenges in the realm of fundamental rights, freedoms of persons and consent. This is important because such technologies have penetrated everyday lives of billions of users - from using Zoom for work meetings, to connecting with others through social media, and beyond.

This is further exacerbated with the emergence of big data and AI technologies, where sensitive information such as geolocation is being gathered and tracked through smartphones, amongst others. Furthermore, even if data is collected legally and with consent, the management, storage and security of data in itself is critical. A watershed moment in this regard is the Cambridge Analytica-Facebook scandal, where data of millions of Facebook users was 'harvested' and sold to buyers, who allegedly range from Donald Trump's 2016 Election campaign, to the Brexit Camp[40]. As it stands, most users (or data subjects) have very poor understanding of the value of their data, of how it is used (or misused) by companies, and/or whether all of this falls under their consent.

According to Privacy International, data protection frameworks "protect people's data by providing individuals with rights over their data, imposing rules on the way in which companies and governments use data, and establishing regulators to enforce the laws.[41]" The idea is to integrate and connect the discourse around digital rights to fundamental rights, with private individuals having access and control over the scope of its usage, and an option to opt out of it - as per their consent. With technologies evolving rapidly, it is essential to introduce legal safeguards, statutes, and laws that outline digital rights of the individual.

Digital Rights Around the World: Examples from the EU and the US

Having charted the scope of cyber surveillance laws in Pakistan, it is useful now to compare it with global best practices, and to review pieces of legislation that progressively integrate data rights amidst the broader discourse of surveillance. The European Union's General Data Protection Regulations (2018) and the California Consumer Privacy Act (CCPA) 2018 provide guidance on not just the scope of rights enjoyed by data subjects, but also introduces safeguards and criminalizes malicious breaches of data while providing remedies to affected users of modern technologies.

---

https://www.pakistantoday.com.pk/2018/08/18/privacy-breach-fears-loom-over-punjab-safe-city-project/

[40] Julia Carrie-Wong, The Cambridge Analytica Scandal Changed the World; But it Didn't Change Facebook, The Guardian, 2019
https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook

[41] Data Protection - Privacy International
https://privacyinternational.org/learn/data-protection

EU: GDPR

The EU's GDPR regime was intended to allow "EU citizens to better control their personal data," as well as update and unify privacy rules allowing businesses to reduce red tape and to benefit from greater consumer trust.[42] The **General Data Protection Regulations (GDPR),** were passed in 2016 and entered into force in 2018. It defines "Personal Data" as "information relating to an identified or identifiable natural person[43]," including sensitive data such as racial or ethnic origin, political opinions, religious beliefs, criminal records, membership of trade unions, genetic and biometric data, health information and data around a person's sex or orientation.[44]

Key Principles

Article 5 of the GDPR lays out seven key principles on how individual data can be handled:[45]

1) Lawfulness, fairness and transparency.
2) Purpose limitation: "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes"
3) Data minimisation: "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed"
4) Accuracy: accurate and kept up to date; every reasonable step must be taken to ensure that inaccurate personal data are erased or rectified without delay.
5) Storage limitation: kept in a form which permits identification of data subjects for no longer than is necessary; it may be stored for longer periods for the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
6) Integrity and confidentiality (security)
7) Accountability

COVID-19 and other emergencies:

Article 9(2)(i) of the GDPR governs emergency powers and lifts the prohibition on any processing of sensitive personal information in the case of "… reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care."[46] Member countries are thereby empowered to adopt temporary rules that expand access while still preserving key GDPR protections.

[42] General Data Protection Regulation – EU (2018) – Summary https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:310401_2
[43] General Data Protection Regulation – EU (2018) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016R0679
[44] Ibid.
[45] Ibid.
[46] Coronavirus Adds an Extra Layer of Challenge to Handling Health Data Under GDPR, CPO Magazine, March 2020. https://www.cpomagazine.com/data-protection/coronavirus-adds-an-extra-layer-of-challenge-to-collection-and-handling-of-health-data-under-the-gdpr/

US: CCPA

The **California Consumer Privacy Act (2018)** or the CCPA covers data protection in the State of California. Passed unanimously, it is regarded as the first law in the United States that frames a comprehensive set of rules around consumer data.

Application and rights:

The CCPA applies to any company that operates in California and either makes at least $25 million in annual revenue, gathers data on more than 50,000 users, or makes more than half its money off of user data. The primary purpose is to create new rights to be exercised by Californian citizens over their data. The most significant categories include "the right to know" (right to be informed) and "the right to say no" (opt out). This enables users to see what data companies have gathered about them, have that data deleted, and opt out of those companies selling it to third parties from now on.

The CCPA does not specifically focus on accountability-related obligations as in the GDPR - instead, CCPA focuses more on transparency obligations, with provisions preventing companies from selling information, providing consumers with the right to opt-out at times of mergers and acquisitions.

In terms of data rights, the CCPA empowers consumers to receive compensation or sue companies, directly for failure of taking action to prevent data breaches. But apart from that, making sure companies comply with the CCPA is the sole province of the attorney general's office, which will only be able to investigate a few cases each year.

Charting Digital Rights under GDPR and CCPA:

The table below compares the scope of rights afforded to data subjects/users under each of the above legislations:

Data Categories	GDPR	CCPA
Right to be Informed/Consent	✓	✓
Right to Access	✓	✓
Right to Portability	✓	✓
Right to Correction	✓	X
Right to Stop Processing/Opt Out	✓	✓
Right to Stop Automated Decision-Making	✓	X
Right to Erasure	✓	✓
Right to equal services and	✓	✓

price		
Private right of suing for damages	X	✓
Regulator enforcement penalties	✓	✓
Emergency provisions (such as for COVID-19)	✓	X (Rules TBD)

Concerns regarding Data Rights in Pakistan

In Pakistan, breaches of data in both the public and private sector are becoming alarmingly frequent. In May 2018, NADRA's CNIC records were hacked while coordinating with the Punjab Information Technology Board to digitize records.[47] The resulting breach saw personal data and other information being sold online by hackers, with no legal recourse provided to individuals who were affected.

Later that year, the Federal Investigation Agency (FIA) confirmed that "almost all" Pakistani banks were hacked in a sophisticated cybersecurity attack, with hackers stealing millions of dollars through debit and credit card information, before further selling the stolen data on the dark web.[48]

As recently as April 2020, a data cache of 115 million Pakistani mobile users was found to be pawned online, with the FIA and PTA leading the investigation into the alleged data breach.[49]

These examples merely present the tip of the iceberg when it comes to the lack of security offered to citizens' data. The use of surveillance techniques (including Big Data/AI) to monitor and collect citizens data in order to pursue an 'infected until proven healthy approach' is, in our view, a necessary response in order to combat the outbreak. However, its use does raise concerns regarding fundamental rights to privacy and therefore needs a legal framework with the requisite procedural safeguards. With medical health records and other geospatial information now being gathered to counter COVID-19, it is critical that elements of data security and protection are integrated into our existing legal framework.

[47] IT Expert Breaks Down How Bad the NADRA Data Breach Was, SAMAA, May 2018. https://www.samaa.tv/news/2018/05/it-expert-breaks-down-just-how-bad-nadra-data-breach-was/
[48] Shakeel Qarar, "Almost all" Pakistani banks hacked in data security breach says FIA, DAWN Nov 2018. https://www.dawn.com/news/1443970
[49] PTA Investigates Data Breach of 115m mobile users, Business Recorder, April 2020. https://www.brecorder.com/2020/04/13/588891/pta-investigates-data-breach-of-115mn-pakistani-mobile-users/

4. Recommendations

These recommendations aim to address potential concerns in undertaking cyber surveillance in Pakistan and suggest mechanisms to ensure such surveillance is conducted while protecting rights to the greatest extent possible:

- Federal and provincial laws should be enacted which establish surveillance powers for the purposes of countering pandemics and allow for information sharing with public health committees. These laws should include safeguards for citizens' privacy and ensure that all data collected is anonymised and pseudonymised and held for only as long as absolutely necessary. A specified upper limit for holding such data should be included in any such legislation.

- The provisions in Punjab and Khyber Pakhtunkhwa's laws which stipulate that the government is to ensure maintenance of secrecy of personal health information and data and not disclose it to any person which may damage the respect, dignity and reputation of citizens are encouraging, however, such provisions should be strengthened in legislation going forward and specific penalties for the breach of privacy or data leaks should be incorporated. They should also establish an authority which can provide oversight and monitor the implementation of these laws. All laws should include a right to a remedy in case of breaches of data privacy in order to promote accountability and transparency.

- The apps and software should be rolled out in accordance with the prescribed legislation or rules framed thereunder. Third parties may be consulted and contracted to provide data analytics services or for technologies for support or surveillance. Any third-party contracts must ensure that these third parties abide by data security protocols when storing data, and that the data must not be processed or otherwise used for purposes other than the original purposes and aims of the contract. There have been cases where this data has either been leaked, sold or used outside the scope of what the data subject had consented to. In such cases, legal recourse must be made available to data subjects to obtain compensation for such breaches, and relevant accountability provisions must be included in the law to ensure all third parties abide by their contracts. A body which can exercise oversight over third parties should be established which is able to adequately scrutinise these entities.

- Mass awareness campaigns must be conducted in which it is emphasised that the data collected will not be misused, repurposed or shared with the private sector without their knowledge or consent. All personal data will be anonymised and deleted once the outbreak is over. In order to facilitate accurate data collection, any public messaging regarding the app will emphasise that the data is being collected for public health reasons and that the submitting of false information will only have adverse health impacts. This will be particularly important for refugee or vulnerable populations who may withhold or submit false information due to fears about their immigration status or other such concerns. These awareness campaigns are important as individuals should be made aware of the laws under which their data is being collected and the objective of this collection. It should also be made clear that measures are being taken to protect privacy and data as far as is possible.

- Citizens may also file freedom of information requests in order to establish whether their personal data is being collected. It should therefore be made clear within the legislation and in the awareness campaigns that all data which is to be collected will be anonymised and no personal identifiers will be used. However, in instances where public authorities have data on a specific individual (for instance, medical records), they should be shared with the requester. This should be done with the understanding that the data was collected due to the highly infectious nature of the disease and the severity of the harm caused by transmission but every effort was made to ensure that non-anonymous data was shared only with the relevant authorities on a strict need-to-know basis and was not made public.

- Other forms of data collection will have to be engaged in for those who do not possess a smartphone perhaps in the form of manual data collectors or paper 'immunity passports' which will perform a similar function in providing access to public services. It should also be emphasised that there will be no penalties for not having a phone or the app and nobody is compelled to upload their data or symptoms or contacts unless necessary by law.

- Technical Advisory Panels should be established which include policy makers, lawyers, and computer scientists and meet regularly in order to review and address issues in the roll out of cyber-surveillance. There should be a form of shared custody of this policy among the relevant stakeholders so that they can share information, inform the strategy and ensure its success.

- Individuals should also have the 'right to be forgotten' even if they were infected with the disease. Legislation should therefore include provisions allowing for data to be deleted beyond a certain time limit and enable individuals to apply for their data to be deleted after the pandemic is over. This could be in part to avoid the stigma of having contracted the virus, this is particularly acute for instance for those in the medical profession, and to protect from future identification as a case.

- In instances where false categorisations have taken place during cyber surveillance, such as when a healthy person has been declared infected (either through faulty data collection, or through flawed automated decision-making via AI), individuals must have the right to rectification and correction of their medical records and other data. Authorities must ensure methods to rectify data records easily and simply, and compensation must be given due to any harm or distress caused by the false categorisation.

- In instances where individuals do not wish for collectors and processors to continue using their data, there must be streamlined mechanisms to allow for individuals to exercise their right to object and withdraw consent. This could happen when information gathered of an infected patient may be pooled with other data to inform policy-making. Safeguards ensuring withdrawal of consent and the use of the right to object must be provided for in the law.

- Forums for remedies should also be ensured in the event of cyber hacks or data breaches. These could take the form of remote tribunals or courts which can hear complaints or grievances about the app or the provision of immunity certificates. A specialised ombudsperson may also be established in which an individual with the appropriate qualifications and expertise in technology law is appointed to hear grievances and make orders. These forums must be given the resources to accept e-petitions and hear complaints through video-conferencing.