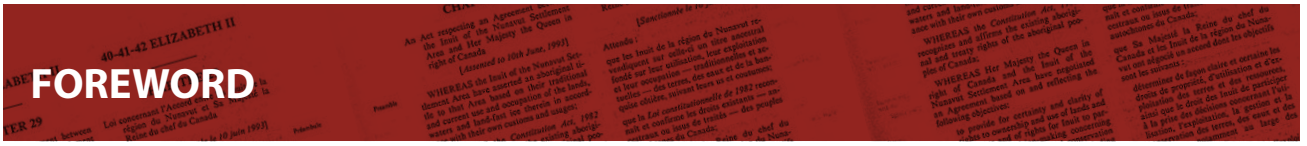
CONFLICTING WITH THE CONSTITUTION

PRIVACY RIGHTS & LAWS IN PAKISTAN

A Bytes for All (B4A), Pakistan Publication,
supported by International Development Research Centre (IDRC) and Privacy International

TABLE OF CONTENTS

TABLE OF CONTENTS



FOREWORD

Be it the Snowden revelations or the growing body of evidence that both national and international governments are involved in heavy surveillance of citizens, there is no longer any doubt that citizen privacy is being compromised in ways that cannot be deemed legal and justified under any circumstances. Pakistan is no different. This report surveys the state of laws and policies in Pakistan that are connected, directly or indirectly with the citizens' right to privacy. This report presents a baseline of laws guiding the exercise of privacy rights in Pakistan and in doing so sets guidelines for relevant stakeholders to set direction for reformative effort.

This report journeys through both national and international laws and conventions and analyze their implications on privacy rights. Over the course of this analysis, it has become abundantly clear that all stakeholders be it the government, the civil society, the corporate sector or the public, need to make urgent and concentrated efforts for legislative reforms that are rights friendly and offer safeguards for this basic right of the citizens.

Based on the in depth analysis of international treaties that Pakistan is a signatory of, and the national legislation that at times impedes on citizen rights, the development and passing of a privacy protection act is recommended. The report also makes various other recommendations particularly the formation of a privacy commission, development of a privacy protection index and the initiation of a mass awareness campaign to guide internet users regarding their privacy rights. The formation of an effective judicial tribunal to deal with privacy intrusion and surveillance has also been recommended. Given the multitude of threats faced by Pakistan, the report also recommends clearly defining the scope of surveillance and limiting it to known terrorist or terrorist organizations who have threatened to wage war against the state and have engaged in or planned to engage in terrorist activities against civilians. The report also calls attention to the lack of an anti-cybercrimes legislation in Pakistan and calls upon the government to revise the existing works in progress to make them human rights based.

This report is a baseline, a first step for encouraging further advocacy efforts on the issue. We urge both the government and the civil society to take the challenge of addressing privacy rights as a serious and urgent priority towards ensuring the civil liberties of the citizens.

Shahzad Ahmad
Country Director
Bytes for All, Pakistan

INTRODUCTION

The growing importance placed upon the right to privacy today can be attributed to technological advancements and stronger interconnectivity within and amongst the nation states around the world. With the advancement of civilization, and the associated growth of civic rights, the concept of privacy has attained substantial importance in legal, political and even philosophical debates. The recognition of privacy as a fundamental right, both nationally and internationally, becomes even more evident when one scrutinizes international treaties, national constitutions and laws. The civil society's formulation of International Principles on Application of Human Rights to Communications Surveillance has further crystallized the concerns that human rights defenders have vis a vis communications surveillance.

Pakistan is a signatory to nearly all international treaties that consider privacy as a fundamental human right, including the UN Declaration of Human Rights and The International Covenant on Civil and Political Right, but excluding the International Convention on the Protection of the Rights of All Migrant Workers and Members of their Families (ICRMW). Furthermore, the 1973 Constitution of Pakistan recognizes the individual's privacy as an inviolable right by specifically guaranteeing the dignity of citizens, privacy of home, the protection of life, liberty and body as fundamental rights. Provisions for privacy are further enunciated in the various laws of the country, subdivided into individual, informational and spiritual domains. These laws, meanwhile, have both positive and negative implications on privacy rights in Pakistan and are, as such, considered the main instrument in this study for understanding the dynamics of privacy in the country. A scrutiny of these laws is essential for devising a set of pragmatic guidelines for stakeholders concerned; said guidelines are also meant to serve as a policy framework on which laws can be evaluated and corrective action taken.

METHODOLOGY

This study was conducted by using three research tools.

a) Literature Review: This was the most extensive phase of the study, during which all international covenants and existing laws were thoroughly scrutinized for their privacy provisions. Three types of documents were reviewed:

a. International and regional covenants;
b. Pakistan's laws;
c. Case laws.

References were also made to Qur'an and Hadith, recognized as sources of law in Islam, to prove that privacy is an inalienable right in religion as well.

b) Focus group discussion with experts in the field, including those from the police, special agencies, PEMRA, and the civil society. The results of this meeting and the ensuing discussion was incorporated in the report.

c) Key Informant interviews: Qualitative in-depth interviews, over the phone and in person, were conducted with legal experts to trace the various laws that might have any association and/or linkages with privacy rights. Due to the lack of explicit legislation for privacy rights in Pakistan, consultations with legal experts were essential in order to formulate an inventory of laws from which to begin our investigation.

STRUCTURE OF THE REPORT

The report is divided into eights sections. **Section A** deals with the conceptual underpinnings of the right to privacy and traces global historical milestones associated therewith. It provides an elaboration of what privacy is and its significance, and identifies the catalog of international conventions that identify privacy as a right. **Sections B to G** are related to the legal status of privacy rights in Pakistan and are the focal point of our investigation. The provisions in sections B to G are further clarified in the comments section and actual case laws have been provided, wherever required, for further elucidation. Finally **Section H** contains concluding remarks and advises a way forward.

How to Read This Report

Each new law in this report has been given an alpha-numeric number. The alphabet denotes the number of the section and the digit denotes the number of the law being discussed in that particular section. Thus A3 means; section A (international treaties), treaty number 3. Similarly, E2 means Section E (miscellaneous laws related to law enforcing agencies) and law number 2. The case laws are expressed in a similar pattern with an abbreviation, CL; thus, CL-E1 means a case law related to law number 1 from section E.

The actual text of the laws is given in *italics*.

SECTION A: PRIVACY IN THE GLOBAL DOMAIN

Understanding Privacy

Of all the human rights in the international catalogue, privacy is perhaps the most difficult to define[1]. The word privacy originates from Latin: "Privatus" that means "separated from the rest or deprived of something"[2].
The Oxford dictionary defines privacy as[3]:

- a state in which one is not observed or disturbed by other people;
- the state of being free from public attention.

Robert Ellis Smith, editor of the Privacy Journal, defined privacy as "the desire by each of us for physical space where we can be free of interruption, intrusion, embarrassment, or accountability and the attempt to control the time and manner of disclosures of personal information about ourselves".

The word in itself is quite comprehensive and includes a broad spectrum of dimensions that are comprised of one or more of the three elements — secrecy, anonymity and solitude — as identified by Ruth Gavison[4]. The concept, however — to delineate the boundaries that mark the access to ones' identity and define the extent to which that identity becomes known to the world around oneself — even when used commonly in daily communication, is not as simple to understand, mainly due to the fact that it has a fundamental role to perform in our daily lives.

Although the notion of privacy varies when we take into account racial, ethnic, societal or temporal changes, the fundamental elements demarcated by Gavison set a baseline for understanding the effects of these variables on privacy requirements. A common principle for guiding nation states in the formulation of country-specific laws is therefore critical for uplifting the standards of living around the world. Recognizing the importance of privacy has, as such, resulted in various global accords that identify privacy as a fundamental human right.

Historical milestones in the recognition of privacy as a right in the international arena:

A1 UN DECLARATION OF HUMAN RIGHTS

The most important of all the international agreements that recognize privacy as a right is the UN Declaration of Human Rights, 1948.

---

1. Privacy and Human Rights 2003: Overview. 2011. Privacy and Human Rights 2003: Overview. [ONLINE] Available at: https://www.privacyinternational.org/survey/phr2003/overview.htm

2. *Related Articles Privacy (from Latin "privatus").* [ONLINE] Available at: http://www.amazines.com/keep_out_related.html. [Accessed 20 Feb 2011]

3. *Definition of privacy from Oxford Dictionaries Online.* [ONLINE] Available at: http://oxforddictionaries.com/view/entry/m_en_gb0662800#m_en_gb0662800. [Accessed 18 Feb 2011]

4. Ruth Gavison, Privacy, 89 yale l.j. 421, 433 (1980)

Article 12

"No-one should be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks on his honour or reputation. Everyone has the right to the protection of the law against such interferences or attacks."

Comments

This article comprehensively defines the dimensions of individual privacy that need to be addressed through country specific laws. The categorization of areas to be considered private for the individual are personal, family, home and correspondence, therefore, including all the facets of a person's identity as well as the social sphere of interaction with the society. The inclusion of the "right to the protection of the law" clearly illustrates the requirement for every country to inculcate lawful provisions guaranteeing this right to be thoroughly administered, with the government serving as the instrument to facilitate the means required.

A2 INTERNATIONAL COVENANT ON CIVIL AND POLITICAL RIGHTS

This convention of 1976 laid great importance to the exercise of "right to privacy", via ***Article 17***, in which the same text as of article 12 of UN Declaration of Human Rights is used to reiterates the internationally-agreed importance laid upon the individual's right to privacy. Pakistan ratified this covenant in June 2010, with a few reservations, none of which have any direct linkages with privacy rights.

A3 CONVENTION ON THE RIGHTS OF THE CHILD

Pakistan ratified the Convention on the Rights of Child (CRC) on December 12, 1990. ***Article 16*** of this convention deals exclusively with the privacy rights of children. The important point to note here is that this convention recognizes children's right to privacy as equal to that of an adult. It therefore demarcates the privacy boundaries of the child as similar to that of an adult by including his or her privacy, family and correspondence within the personal privacy domains. This article also takes into account a child's honor and reputation under privacy rights by prohibiting any unlawful attacks thereon. It further establishes right to protection of law for the child with regard to his or her privacy rights.

Article 16

> *1. No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, or correspondence, nor to unlawful attacks on his or her honour and reputation.*
>
> *2. The child has the right to the protection of the law against such interference or attacks.*

A4 INTERNATIONAL CONVENTION ON THE PROTECTION OF THE RIGHTS OF ALL MIGRANT WORKERS AND MEMBERS OF THEIR FAMILIES (ICRMW)

This convention was adopted by General Assembly's resolution 45/158 of December 18, 1990. ICRMW adds another dimension to privacy rights by granting migrant workers and their families, protection similar to citizens of the country to which they migrate. This convention is very important in extending the horizon of the

privacy domain to cover all people residing in a country, whether citizens or migrants, with equality. Pakistan has neither signed nor ratified ICRMW, even though the Convention is vital for keeping abreast of global trends in strengthening privacy rights.

Article 14 of the convention deals with privacy rights granted in language that is similar to the international conventions mentioned earlier:

Article 14

No migrant worker or member of his or her family shall be subjected to arbitrary or unlawful interference with his or her privacy, family, correspondence or other communications, or to unlawful attacks on his or her honour and reputation. Each migrant worker and member of his or her family shall have the right to the protection of the law against such interference or attacks.

Regional Efforts on Privacy Rights

Along with the aforementioned international conventions which having a global scope, there are also agreements pertaining to human rights that signify privacy rights amongst regional groupings. Although Pakistan is not a member of any of these regional agreements, these agreements are presented below in order to recognize the fact that human rights, and privacy rights in particular, are given due importance in diversified cultures, religions, and geographical localities:

A5 EUROPEAN CONVENTION FOR THE PROTECTION OF HUMAN RIGHTS (ECHR)

The ECHR was adopted in Rome on November 4, 1950. This convention has five protocols, although the section on privacy rights was identified at the time of origin in ***Article 8***:

> *1. Everyone has the right to respect for his private and family life, his home and his correspondence.*
>
> *2. There shall be no interference by a public authority with the exercise of this right except as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health of morals, or for the protection of the rights and freedoms of others.*

Comments

Similar to other international conventions, the ECHR lays down private, family life, home and correspondence as domains that are demarcated as private for individuals. This convention extends further and delineates the areas that are considered exceptions such as interests of national security, public safety, the economic well-being of the country for the prevention of disorder and crime, for the protection of health or morals of others, or for the protection of the rights and freedoms of others. This convention is very important as it helps in identifying the areas (exceptions) falling out of the domain of privacy.

A6 CAIRO DECLARATION ON HUMAN RIGHTS IN ISLAM (CDHRI)

CDHRI is a declaration of the member states of the Organization of Islamic Conference (OIC), Adopted in Cairo in 1990, the CDHRI provides an overview of Islamic perspective on human rights. The Declaration starts by forbidding (in terms of basic human dignity and basic obligations and responsibilities) "discrimination on the basis of race, color, language, belief, sex, religion, political affiliation, social status or other considerations". It continues on to proclaim the sanctity of life and "preservation of human life" as "a duty prescribed by Shariah". The Cairo declaration very explicitly declares privacy as a right. ***Article 18*** of this declaration is reproduced below:

> *a. Everyone shall have the right to live in security for himself, his religion, his dependents, his honor and his property.*
>
> *b. Everyone shall have the right to privacy in the conduct of his private affairs, in his home, among his family, with regard to his property and his relationships. It is not permitted to spy on him, to place him under surveillance or to besmirch his good name. The State shall protect him from arbitrary interference.*
>
> *c. A private residence is inviolable in all cases. It will not be entered without permission from its inhabitants or in any unlawful manner, nor shall it be demolished or confiscated and its dwellers evicted.*

A7 ARAB CHARTER ON HUMAN RIGHTS

The Arab Charter on Human Rights was adopted by the Council of the League of Arab States on May 22, 2004 and affirms the principles contained in the UN Charter, the Universal Declaration of Human Rights, the International Covenants on Human Rights, and Cairo Declaration on Human Rights in Islam[5]. It has been in force since March 15, 2008. A number of traditional human rights are provided for, including the right to liberty and security of persons, the equality of persons before the law, the protection of persons from torture, the right to own private property, the freedom to practice religious observance and freedom of peaceful assembly and association. The Charter also recognizes privacy as a right. ***Article 17*** states:

Privacy shall be inviolable and any infringement thereof shall constitute an offence. This privacy includes private family affairs, the inviolability of the home and the confidentiality of correspondence and other private means of communication.

A8 13 PRINCIPLES

The work on these principles began in October 2012 at a meeting of more than 40 privacy and security experts in Brussels. After an initial broad consultation, which included a second meeting in Rio de Janeiro in December 2012, Access, EFF and Privacy International led a collaborative drafting process that drew on the expertise of human rights and digital rights experts across the world. The first version of the Principles was finalised on 10 July 2013, and officially launched at the UN Human Rights Council in Geneva in September 2013. The resounding success and global adoption of the Principles by more than 400 organisations across the world necessitated a number of specific, primarily superficial textual changes in the language of the

5. *Human Rights in Arab Countries: Bridging the Gulf.* [ONLINE] Available at: http://www.bridgingthegulf.org/links/human-rights-ngos.html. [Accessed Feb 26, 2011]

Principles in order to ensure their consistent interpretation and application across jurisdictions. The final version was released in May, 2014.

- ***LEGALITY:*** *Any limitation to human rights must be prescribed by law. The State must not adopt or implement a measure that interferes with these rights in the absence of an existing publicly available legislative act, which meets a standard of clarity and precision that is sufficient to ensure that individuals have advance notice of and can foresee its application. Given the rate of technological changes, laws that limit human rights should be subject to periodic review by means of a participatory legislative or regulatory process.*

- ***LEGITIMATE AIM:*** *Any limitation to human rights must be prescribed by law. The State must not adopt or implement a measure that interferes with these rights in the absence of an existing publicly available legislative act, which meets a standard of clarity and precision that is sufficient to ensure that individuals have advance notice of and can foresee its application. Given the rate of technological changes, laws that limit human rights should be subject to periodic review by means of a participatory legislative or regulatory process.*

- ***NECESSITY:*** *Surveillance laws, regulations, activities, powers, or authorities must be limited to those which are strictly and demonstrably necessary to achieve a legitimate aim. Communications Surveillance must only be conducted when it is the only means of achieving a legitimate aim, or, when there are multiple means, it is the means least likely to infringe upon human rights. The onus of establishing this justification is always on the State.*

- ***ADEQUACY:*** *Any instance of Communications Surveillance authorised by law must be appropriate to fulfil the specific Legitimate Aim identified.*

- ***PROPORTIONALITY:*** *Communications surveillance should be regarded as a highly intrusive act that interferes with human rights threatening the foundations of a democratic society. Decisions about Communications Surveillance must consider the sensitivity of the information accessed and the severity of the infringement on human rights and other competing interests. This requires a State, at a minimum, to establish the following to a Competent Judicial Authority, prior to conducting Communications Surveillance for the purposes of enforcing law, protecting national security, or gathering intelligence.*

- ***COMPETENT JUDICIAL AUTHORITY:*** *Determinations related to Communications Surveillance must be made by a competent judicial authority that is impartial and independent.*

- ***DUE PROCESS:*** *Due process requires that States respect and guarantee individuals' human rights by ensuring that lawful procedures that govern any interference with human rights are properly enumerated in law, consistently practiced, and available to the general public. Specifically, in the determination on his or her human rights, everyone is entitled to a fair and public hearing within a reasonable time by an independent, competent and impartial tribunal established by law, 10 except in cases of emergency when there is imminent risk of danger to human life. In such instances, retroactive authorisation must be sought within a reasonably practicable time period. Mere risk of flight or destruction of evidence shall never be considered as sufficient to justify retroactive authorisation.*

- ***USER NOTIFICATION:*** *Those whose communications are being surveilled should be notified of a decision authorising Communications Surveillance with enough time and information to enable them to challenge the decision or seek other remedies and should have access to the materials presented in support of the application for authorisation.*

• ***TRANSPARENCY:*** *States should be transparent about the use and scope of Communications Surveillance laws, regulations, activities, powers, or authorities. They should publish, at a minimum, aggregate information on the specific number of requests approved and rejected, a disaggregation of the requests by service provider and by investigation authority, type, and purpose, and the specific number of individuals affected by each. States should provide individuals with sufficient information to enable them to fully comprehend the scope, nature, and application of the laws permitting Communications Surveillance. States should not interfere with service providers in their efforts to publish the procedures they apply when assessing and complying with State requests for Communications Surveillance, adhere to those procedures, and publish records of State requests for Communications Surveillance.*

• ***PUBLIC OVERSIGHT:*** *States should establish independent oversight mechanisms to ensure transparency and accountability of Communications Surveillance.11 Oversight mechanisms should have the authority: to access all potentially relevant information about State actions, including, where appropriate, access to secret or classified information; to assess whether the State is making legitimate use of its lawful capabilities; to evaluate whether the State has been comprehensively and accurately publishing information about the use and scope of Communications Surveillance techniques and powers in accordance with its Transparency obligations; to publish periodic reports and other information relevant to Communications Surveillance; and to make public determinations as to the lawfulness of those actions, including the extent to which they comply with these Principles. Independent oversight mechanisms should be established in addition to any oversight already provided through another branch of government.*

• ***INTEGRITY OF COMMUNICATIONS AND SYSTEMS: I****n order to ensure the integrity, security and privacy of communications systems, and in recognition of the fact that compromising security for State purposes almost always compromises security more generally, States should not compel service providers or hardware or software vendors to build surveillance or monitoring capability into their systems, or to collect or retain particular information purely for State Communications Surveillance purposes. A priori data retention or collection should never be required of service providers. Individuals have the right to express themselves anonymously; States should therefore refrain from compelling the identification of users.*

• ***SAFEGUARDS FOR INTERNATIONAL COOPERATION:*** *In response to changes in the flows of information, and in communications technologies and services, States may need to seek assistance from foreign service providers and States. Accordingly, the mutual legal assistance treaties (MLATs) and other agreements entered into by States should ensure that, where the laws of more than one state could apply to Communications Surveillance, the available standard with the higher level of protection for individuals is applied. Where States seek assistance for law enforcement purposes, the principle of dual criminality should be applied. States may not use mutual legal assistance processes and foreign requests for Protected Information to circumvent domestic legal restrictions on Communications Surveillance. Mutual legal assistance processes and other agreements should be clearly documented, publicly available, and subject to guarantees of procedural fairness.*

• ***SAFEGUARDS AGAINST ILLEGITIMATE ACCESS AND RIGHT TO EFFECTIVE REMEDY:*** *States should enact legislation criminalising illegal Communications Surveillance by public or private actors. The law should provide sufficient and significant civil and criminal penalties, protections for whistleblowers, and avenues for redress by those affected. Laws should stipulate that any information obtained in a manner that is inconsistent with these principles is inadmissible as evidence or otherwise not considered in any proceeding, as is any evidence derivative of such information. States should also enact laws providing that, after material obtained through Communications Surveillance has been used for the purpose for which information was given, the material must not be retained, but instead be destroyed or returned to those affected.*

SECTION B: PRIVACY AS A RIGHT IN PAKISTAN

B1 CONSTITUTION OF PAKISTAN, 1973

Article 4 (reproduced below) of the 1973 Constitution recognizes the right of every citizen and of every other person for the time being within the Country to be protected and treated in accordance with law.

Right of individuals to be dealt with in accordance with law, etc.

1. To enjoy the protection of law and to be treated in accordance with law is the inalienable right of every citizen, wherever he may be, and of every other person for the time being within Pakistan.

2. In particular:

a) no action detrimental to the life, liberty, body, reputation or property of any person shall be taken except in accordance with law;

b) no person shall be prevented from or be hindered in doing that which is not prohibited by law; and

c) no person shall be compelled to do that which the law does not require him to do.

Comments

Article 4 (2) disallows any action detrimental to the life, liberty, body, reputation or property of any person to be taken except in accordance with law. If we closely examine each factor outlined in ***Article 4 (2)*** separately, we recognize that privacy has strong direct and indirect associations with all of them. For example, when we talk about the life of a person it includes not just the quantitative element of longevity but also include the qualitative aspects that mark his/her existence as a human being. "Privacy is the bedrock of freedom", therefore liberty of individuals is mainly dependent upon allowing them to exercise the right of privacy. The body, reputation or property of person are all closely associated with privacy[6] and have strong linkages thereof.

The 1973 constitution extends further in the section "fundamental rights" to reiterate the huge importance given to life and liberty in Pakistan. The ***Article 9*** states:

Security of person

"No Person shall be deprived of life or liberty save in accordance with law"

The constitution doesn't stop here; it clearly identifies the right to privacy of a person and the inviolability of dignity of every person in Pakistan to be a fundamental right, thus guaranteeing the privacy of home.

Article 14 (1) Inviolability of dignity of man

"The dignity of man, subject to law, the privacy of home, shall be inviolable"

6. R, Volkman, 2003. Privacy as life, liberty, property. 5th ed. Hingham: Kluwer Academic Publishers

The notion of privacy is closely linked to dignity of a person as there are a lot of aspects of personal life that a person does not want to be made public and which is not required to be made public as dignity is recognized as a fundamental right in the constitution.

It should be noted that the Constitution provides the requisite framework on which the country's laws are based on or derived from. It is a parent document supporting the birth of the sub-documents that govern the laws, rules and regulations of a country. These laws, rules and regulations can either be general, i.e. having an impact on every person in the country (such as the Pakistan Penal Code of 1860 and the Freedom of Information Ordinance 2002), or sector-specific (such as the Press Council of Pakistan Ordinance of 2002, the Banking Companies Rules of 1963, and the PM&DC code of ethics). On whatever tier the law is enunciated, the effectiveness of the devised law is dependent upon its submission to the parent document, i.e. the 1973 Constitution of Pakistan. No law, rule or regulation of Pakistan can, in any case, be in direct or indirect contradiction to the Constitution.

The Constitution, meanwhile, clearly states in ***Article 8*** that laws that are inconsistent or in derogation of fundamental rights to be void, except in the case of laws relating to the armed forces, or to the police for the maintenance of public order, proper discharge of their duties or of maintenance of discipline among them.

Article 8 of the 1973 Constitution states:

Laws inconsistent with or in derogation of fundamental rights to be void

> *1. Any law, or any custom or usage having the force of law, in so far as it is inconsistent with the rights conferred by this Chapter, shall, to the extent of such inconsistency, be void.*
>
> *2. The State shall not make any law which takes away or abridges the rights so conferred and any law made in contravention of this clause shall, to the extent of such contravention, be void.*
>
> *3. The provisions of this Article shall not apply to:*
> *a) any law relating to members of the Armed Forces, or of the police or of such other forces as are charged with the maintenance of public order, for the purpose of ensuring the proper discharge of their duties or the maintenance of discipline among them;*

Comments

The only point of concern in ***Article 8*** is the section 3 (a) that the provisions of the article do not apply to armed forces and police etc for the maintenance of public order or for the purpose of ensuring the proper discharge of their duties. However, the powers and sphere of influence of these authorities, especially police, is clearly defined in their respective rules and regulations.

The 1973 constitution of Pakistan considers Islamic rules and principles as fundamental elements to guide the development of law in the country. ***Article 227*** specifically obliges the state to develop laws in accordance with Islamic teachings and restricts the development of any law that is not as per the teachings of Quran and Sunnah. ***Article 227*** states:

Provisions relating to the Holy Quran and Sunnah

(1) All existing laws shall be brought in conformity with the Injunctions of Islam as laid down in the Holy Quran and Sunnah, in this Part referred to as the Injunctions of Islam, and no law shall be enacted which is repugnant to such injunctions.

Comments

When we speak about privacy, we find that the Quran and Sunnah have an inventory of references that can play a key role in clarifying our understanding of Privacy Rights as guaranteed in Islamic teachings. This enables us to develop a standard to gauge the application of Islamic Privacy principals in Pakistan and see for ourselves how thoroughly they have been entwined and observed.

The Quran speaks explicitly about privacy rights with particular reference to the privacy of the home and the procedure of entrance in the following verse:

> "O ye who believe! Enter not houses other than your own until you have asked leave and saluted the inmates thereof. That is better for you, that you may be heedful. And if you find no one therein, do not enter them until you are given permission. And if it be said to you, `Go back then', then go back; that is purer for you. And Allah knows well what you do."[7]

At another place the Quran abhors spying on another; an important aspect to ensure that privacy of a person is not violated by another:

> "O ye who believe! avoid most of suspicions; for suspicion in some cases is a sin. And spy not on each other, nor back-bite one another. Would any of you like to eat the flesh of his brother who is dead? Certainly you would loathe it. And fear Allah, surely Allah is Oft-Returning with compassion and (is) Merciful."[8]

There are also authentic records of instances that have occurred during the life of the Holy Prophet (pbuh) that set a guiding framework with reference to ensuring the privacy of individuals in their homes:

> "It is reported that a man came to see Prophet Muhammad, peace be upon him, and sought permission for entry while standing just in front of the door. The Prophet said to him; "Stand aside: the object of the Commandment for seeking permission is to prevent casting of looks inside the house."[9]

The procedure for entry to another person's residence is also evident from the Prophet Muhammad's (pbuh) personal life:

> "The practice of the Prophet, peace and blessings be upon him, was that whenever he went to see somebody, he would stand aside, to the right or the left of the door, and seek permission as it was not then usual to hang curtains on the doors."[10]

Sahl b. Sa'd as-Sa'id reported that a person peeped through the hole of the door of Allah's Messenger (may peace be upon him), and at that time Allah's Messenger (may peace be upon him) had with him a scratching

---

7. (An-Noor, 24:27-28)

8. (Al-Hujuraat, 49:12)

9. (Abu Da'ud Book 41, Number 5155)

10. (Abu Da'ud Book 8, Number 5167)

instrument with which he had been scratching his head. When Allah's Messenger (may peace be upon him) saw him. he said: If I were to know that you had been peeping through the door, I would have thrust that into your eyes, and Allah's Messenger (may peace be upon him) said: Permission is needed as a protection against glance[11].

Islam has placed similar sanctity to the privacy of data. There are also references to ensuring the data privacy of an individual and more specifically correspondence in the teachings of the Holy Prophet (pbuh):

> "According to Hadrat Abdullah bin Abbas, the Prophet said; 'Whoever glances through the letter of his brother without his permission, glances into fire.'"[12]

Another source of inspiration is the conduct of the companions of the Holy Prophet (pbuh) and in this respect the incident of Caliph Hazrat Umar (R.A.) is often quoted when he during the routine nocturnal patrolling, heard a woman singing in her house. The Caliph, the head of the government, scaled the wall and saw her enjoying liquor. As the story goes, the inmate of the house on the contrary charged the Caliph of violating three injunctions: (a) spying, (b) entry in the house by scaling instead of coming from the front door and (c) forcing entry in the house (of course without permission). The Caliph did not take cognizance of the offence because the privacy of the house was inviolable and the law protected it. The Caliph did not prosecute the culprit either even though he was an eye witness because he was not a natural witness and had witnessed the incident taking place in the house only after scaling the wall which was not permissible. It is worth noting that the inmate of the house was not disturbing public peace.

Recognizing the fact that no law in the country can be made that defy Islamic principles and having the understanding thereof, we shall now move our focus to more specific Pakistani legal instruments in the subsequent section.

11. (Sahih Muslim Book 025, Number 5366)

12. (Abu Da'ud Book 8, Number 1480)

SECTION C: INVENTORY OF PAKISTANI LAWS WITH REFERENCE TO PRIVACY

C1 PAKISTAN PENAL CODE (ACT XLV OF 1860)[13]

The PPC is the primary laws for all offences charged in Pakistan. It is applicable across the country and has been in force since the birth of the nation, with a few modifications per Islamic principles.

PPC and Criminal Trespass

The section on criminal trespass is very comprehensive and ensures that the privacy of home remains under the protection of the law. This section constitutes either illegal entry or legal entry followed by illegal stay as categories of criminal trespass. The intent of the trespasser is also comprehensively defined; it includes trespassing for the sake of offense, to intimidate, insult or annoy. Staying longer then lawfully required is also categorized under intent. There are also categories that define trespassing under various reasons and conditions along with their appropriate explanations and respective punishments. This section comprises ***Articles 441-462***, as given below:

441. Criminal trespass

Whoever enters into or upon property in the possession of another with intent to commit an offence or to intimidate, insult or annoy any person in possession of such property, or, having lawfully entered into or upon such property, unlawfully remains there with intent thereby to intimidate, insult or annoy any such person, or with intent to commit an offence, is said to commit "criminal trespass".

442. House-trespass

Whoever commits criminal trespass by entering into or remaining in any building, tent or vessel used as a human dwelling or any building used as a place for worship, or as a place for the custody of property, is said to commit "house-trespass".

443. Lurking house-trespass

Whoever commits house-trespass having taken precautions to conceal such house-trespass from some person who has a right to exclude or eject the trespasser from the building, tent or vessel which is the subject of the trespass, is said to commit "lurking house-trespass".

444. Lurking house-trespass by night

Whoever commits lurking house-trespass after sunset and before sunrise, is said to commit "lurking house-trespass by night".

---

13. *Pakistan Penal Code (Act XLV of 1860).* [ONLINE] Available at: http://www.pakistani.org/pakistan/legislation/1860/actXLVof1860.html. [Accessed 26 May 2011]

A person is said to commit "house-breaking" who commits house-trespass if he effects his entrance into the house or-any part of it in any of the six ways hereinafter described; or if, being in the house or any part of it for the purpose of committing an offence, or, having committed an offence therein, he quits the house or any part of it in any of such six ways, that is to say:

First: *If he enters or quits through a passage made by himself, or by any abettor of the house-trespass, in order to the committing of the house-trespass.*

Secondly: *If he enters or quits through any passage not intended by any person, other than himself or an abettor of the offence, for human entrance; or through any passage to which he has obtained access by scaling or climbing over any wall or building.*

Thirdly: *If he enters or quits through any passage which he or any abettor of the house-trespass has opened, in order to the committing of the house-trespass by any means by which that passage was not intended by the occupier of the house to be-opened.*

Fourthly: *If he enters or quits by opening any lock in order to the committing of the house-trespass, or in order to the quitting of the house after a house-trespass.*

Fifthly: *If he effects his entrance or departure by using criminal force of committing an assault, or by threatening any person with assault.*

Sixthly: *If he enters or quits any passage which he knows to have been fastened against such entrance or departure, and to have been fastened by himself or by an abettor of the house-trespass.*

446. House-breaking by night

Whoever commits house-breaking after sunset and before sunrise, is said to commit "housebreaking by night."

447-462 deals with the various sorts of punishments associated with trespassing in individually

Comments

We consider all forms of trespassing for whatsoever intent, in addition to the ones enumerated in section 441, as intrusion into the privacy of the home. Further elaboration of intent of entry is vital in order to classify it under different crimes and to prescribe different punishments. We will, however, not be discussing those as our only concern here was to elaborate the PPC's extensive mechanism to address criminal trespass. That said, we believe that this section has been developed to directly redress criminal trespass and having indirect linkages with privacy. It shall encompass trespass into private property for any intent other than the ones mentioned as a violation of the right to privacy and the inviolability of the home, and therefore, a crime on its own. We consider it necessary as there might be cases where the intent of the first entry was not of any offense as characterized under the intent section (such as getting a cricket ball from the house without permission from the owner); however, once the information about private property has been collected it can be used to assist crime. The violation of the private property's boundary should therefore be considered a crime in itself, even though the intent of the first entry was not criminal; unless authorized by the owner of the property to do so.

C2 DEFAMATION ORDINANCE 2002/ DEFAMATION BILL 2004

The Defamation Ordinance of 2002[14] has replaced Clause 499 of the PPC that dealt with defamation. The defamation law of Pakistan is supported by the Defamation Ordinance of 2002 and the successive Defamation Bill of 2004.

The ***Article 3*** of the ordinance defines defamation as follows:

3. Defamation

> *1. any wrongful act or publication or circulation of a false statement or representation made orally or in written or visual form which injures the reputation of a person, tends to lower him in the estimation of others or tends to reduce him to ridicule, unjust criticism, dislike, contempt or hatred shall be actionable as defamation.*
>
> *2. Defamation is of two forms, namely:*
> *(i) slander; and*
> *(ii) libel.*
>
> *3. Any false oral statement or representation that amounts to defamation shall be actionable as **slander**.*
>
> *4. Any false written, documentary or visual statement or representation made either by ordinary form or expression or by electronic or other modern means or devices that amounts to defamation shall be actionable as **libel**.*

Comments

The five-page defamation ordinance, focusing specifically on defamation, should have been made more extensive and comprehensive in terms of providing safeguards for the individual's interests. In fact, this ordinance, has been made less illustrative, and as such, less effective than the prior penal code's section on defamation that included clear illustrations of exceptions to defamation.

CL-C2 | Case law: 2010 YLR 1647 KARACHI-HIGH-COURT-SINDH

> **Side Appellant:** SHARIQ SAEED
> **Side Opponent:** MANSOOB ALI KHAN

S.3---Constitution of Pakistan (1973), Arts. 14 & 19---Defamation---Dignity of man---Freedom of speech---Principles---Freedom of expression is one of those fundamental rights which are considered to be the corner stone of democratic institutions---Right of free speech extends to all subjects which affects way of life without limitation of any particular fact of human interest and includes in the main term 'freedom of expression'---Right of freedom of speech and expression carries with it the right to publish and circulate one's idea, opinion and views with complete freedom and by resorting to any available means of publication---Right of freedom of speech and expression is not unfettered and unbridled---Absolute and unrestricted such individual rights do not exist in any modern State and there is no such thing as absolute and uncontrolled liberty---While allowing freedom of speech and expression as a fundamental right, it is also provided under Art. 14 of the Constitution, that dignity of man, subject to law, the **privacy** of home are inviolable---Such principle is

14. 2011 [ONLINE] Available at: http://www.intermedia.org.pk/mrc/medialawdocs/defamation-law.pdf. [Accessed 26 May 2011]

required to be extended further to the case where any defamation is caused, because human dignity, honor and respect is more important than comforts and necessities---No attempt on the part of any person individually, jointly or collectively to detract, defame or disgrace other person, thereby diminishing, decreasing and de-grading dignity, respect, reputation and value of life---Provisions of Art. 14 of the Constitution, providing for dignity of man as a fundamental right, is the most valuable right---Dignity of man is not only provided by Constitution of Pakistan, but according to history and under Islam, great value has been attached to dignity of man and **privacy** of home---While exercising right of freedom of speech and expression, one has to keep in his mind that he has also a corresponding responsibility and duty to ensure that his freedom of expression or speech may not transgress limits of freedom beyond the boundaries of Art. 14 of the Constitution.

C3 FREEDOM OF INFORMATION ORDINANCE 2002[15]

The right to information is considered a fundamental right under the UN Declaration of Human Rights. Its primary aim is to ensure greater transparency and accountability in government departments, thus elevating the standards of governance in the country. While freedom of information might seem contradictory to the right to privacy, it should be noted that privacy as a concept is applicable to individuals and citizens and not government departments. As the government holds a large database of citizen's personal information related to different spheres, however, it is critical that a line be drawn regarding what level of information cannot be supplied by government departments under this ordinance. The demarcation identified under this ordinance, in ***Article 8***, has three provisions with respect to privacy: exclude records of banking companies and financial institutions relating to customer accounts ***(8 d)*** are excluded, as are records relating to the personal privacy of individuals ***(8 g)***, and records of private documents furnished to a public body ***(8 h).*** The relevant text of the ordinance is as follows:

8. Exclusion of certain record. - Nothing contained in section 7 (provides a list of public record) shall apply to the following record of all public bodies, namely:

> *(d) record of the banking companies and financial institutions relating to the accounts of their customers;*
>
> *(g) record relating to the personal privacy of any individual;*
>
> *(h) record of private documents furnished to a public body either on an express or implied condition that information contained in any such documents shall not be disclosed to a third person*

There are also provincial laws related to freedom of information in Balochistan (2005)[16] and Sindh (2006)[17] that set similar boundaries with regards to individual privacy per the federal ordinance.

---

15. Pakistan - Freedom of Information Ordinance 2002. 2011. *Pakistan - Freedom of Information Ordinance 2002.* [ONLINE] Available at: https://www.privacyinternational.org/countries/pakistan/pk-foia-1002.html. [Accessed 26 May 2011]

16. *Balochistan FOI Law - Campaign for Freedom of Information, Pakistan.* [ONLINE] Available at: http://www.ourrighttoknow.org/balochistan-foi-law.html. [Accessed 26 May 2011]

17. *Sindh FOI Law - Campaign for Freedom of Information, Pakistan.* [ONLINE] Available at: http://www.ourrighttoknow.org/sindh-foi-law.html. [Accessed 26 May 2011]

SECTION D: TERRORISM AND PRIVACY

Although terrorism has been a long prevailing peril for Pakistan, a massive upsurge in terrorist incidents has also been notably evident since the US 9/11 attacks. This increase is mainly attributed to the high involvement of Pakistan as a front line state in the war against terrorism, which has further divided Pakistan along ideological, ethnic, provincial and socio-cultural fronts. This has amplified the state of insecurity and extremism in the country, leading to the loss of precious lives. Per the South Asia Terrorism Portal database, there have been 9,620 civilian and 3,443 security forces fatalities due to terrorism in Pakistan from 2003 to February 20, 2011[18]. The yearly trends depict that causalities related to terrorism have been on a continuous rise since 2003. As a result of this, fear and a high level of concern is widespread in the general public. According to the Pew Global Attitudes survey released on July 29, 2010, 98% of those surveyed in Pakistan consider terrorism as a very big problem for the country[19].

As such, both, the magnitude and intensity of terrorism is immensely severe; it can range from physical losses such as those to life and property of individuals to much broader psychological implications by instilling a constant state of fear and panic in the public. Unanimity of opinion regarding the economic loss suffered by nation due to terrorism is also evident in popular research literature. International and national conventions, laws and regulations, meanwhile, allow for the infringement of privacy to carry out lawful procedures; explicitly stated in Pakistani laws for reasons such as the protection of national security, avoidance of economic losses and prevention of disorder in society, to name a few. Considering the fact that the implications of terrorism are linked directly with the aforementioned areas, and that Pakistan's global ranking per the 2010 report of Maplecroft's Terrorism Risk Index is second in the world , there is a need to devise comprehensive laws regarding terrorism in order to ensure that a just and accountable system is established, with all requisite judicial checks, and which has a clear delineation of the power limits of every agency, while maintaining a strict balance with privacy rights.

D1 ANTI TERRORISM ACT 1997[21]

While the major law governing the country with respect to terrorism is the Anti-Terrorism Act of 1997, anti-terrorism law has existed in Pakistan since the birth of the country. The initial legal instrument dealing with terrorism was Section 144 of the Criminal Procedure Code (CrPC). It was replaced in 1975 with the Terrorist Activities Act, and finally the 1997 Anti-Terrorism Act was promulgated in an attempt to curb terrorism in the country. The Anti-Terrorism Act of 1997 was an attempt to impart timely and inexpensive justice by establishing

18. *Pakistan Assessment 2011*. [ONLINE] Available at: http://www.satp.org/satporgtp/countries/pakistan/. [Accessed 8 Mar 2011]

19. *Concern About Extremist Threat Slips in Pakistan | Pew Global Attitudes Project*. [ONLINE] Available at: http://pewglobal.org/2010/07/29/concern-about-extremist-threat-slips-in-pakistan/. [Accessed 15 Mar 2011]

20. *Review of Maplecroft's "Terrorism Risk Index 2011" | Terrorism*. [ONLINE] Available at: http://terrorism.foreignpolicyblogs.com/2010/12/04/review-of-maplecrofts-%E2%80%9Cterrorism-risk-index-2011%E2%80%9D/. [Accessed 15 Mar 2011]

21. 2011 [ONLINE] Available at: http://www.fmu.gov.pk/docs/laws/The%20Anti%20Terrorism%20Act.pdf. [Accessed 26 May 2011]

a parallel legal system. The 1997 version was further modified over time to include various other clauses and definitions, most of which have been criticized by the media and scholarly circles for extending the powers of the ruling regimes.

Keeping our focus intact, following are the provisions found to be related with privacy rights in the Anti-Terrorism Act:

5. Use of armed forces and civil armed forces to prevent terrorism

(2) In particular and without prejudice to the generality of the provisions of sub-section (1), an officer of the police, armed forces and civil armed forces may---
iii) Enter and search without warrant, any premises to make any arrest or to take possession of any property, fire-arm, weapon or article used or likely to be used, in the commission of any terrorist act or scheduled offence

Comments

The powers given to officers of law-enforcing agencies per the Article, open up venues for the exploitation of power because the Article in question does not require that an evidence of suspicion be presented to the court to seek permission before entering and searching any premises.

10. Power to enter or search

If an officer of the police, armed forces or civil armed forces is satisfied that there are reasonable grounds for suspecting that person has possession of written material or a recording in contravention of section he may enter and search the premises where it is suspected the material or recording is situated and take possession of the same.

Comments

This article allows officers of law-enforcing agencies the power of entering and searching premises, and taking possession of written or recorded material if there are reasonable grounds for suspecting that possession of written or recorded material in contravention of section exists (defined under terrorism). We believe that the this article should include the requirement that the entering officer present a written statement to the individual under suspicion as to why the officer believes that said individual is being investigated and also submit the same to the court beforehand.

Another area of great concern is the role of intelligence agencies in covert surveillance operations across the country. The problem is augmented due to the fact that there is no law governing the creation or operation of these intelligence agencies. Thus, the operational powers and jurisdiction of these intelligence agencies are not confined by any legal delineations. In the absence of support of law for power demarcation, intelligence agencies, including the ISI and MI, have been used in Pakistan for the attainment of political motives of the federal government, mostly during the reigns of military dictators.

As such, the undefined powers of intelligence agencies, coupled with major loopholes in the legal instruments governing Pakistan are a notable impediment in bestowing Pakistani citizens with their fundamental privacy rights. We would now take our quest further by exploring Acts that deal directly with the violation of privacy for reasons of safeguarding national interest.

D2 SECURITY OF PAKISTAN ACT, 1952

This act was enacted to provide special measures for dealing with persons acting in a manner prejudicial to the defense, external affairs and security of Pakistan.

Section Three of the Act provides the reasons and crimes under which this Act will be applicable and then illustrate in ***(1) (e)*** the intrusion of that person's privacy as made permissible through this Act:

3---(1) The Federal government if satisfied with respect to any particular person, that, with a view to preventing him from acting in any manner prejudicial to the defense or external affairs or the security of Pakistan or any part thereof, it is necessary so to do, may make an order

> *(e) Requiring him to notify his movements or to report himself or both notify his movements and report himself in such manner, at such times, and to such authority or person, as may be specified in the order;*

Comments

We believe that the absence of any illustrations or examples of the three types of crimes as mentioned in ***3---(1)*** is a major loophole that diminishes the public's confidence in this Act being devised pragmatically. Here again, the power of discretion to identify as guilty or not is held by the federal government rather than the judiciary. Without the presence of adequate illustrations to exemplify these categories of crime, the justifications for accusing someone become limitless and therefore, the scope can be enhanced whenever and wherever required for individual or political motives. Secondly, that person is required to act in eight ways, listed from 'a' to 'h', wherein point 'e' has direct linkages with privacy rights, i.e. the accused has to report his/her movements and/or to report herself/himself in a particular manner, at particular times, and to a particular authority or person, as might be specified in the order. Firstly, the area of movement (whether said movement is restricted to the city or just to the market across the street) is not known, and if the magnitude of movement is tilted towards the latter, then it is almost like being imprisoned. Furthermore, the addition of a multitude of variations as to whom, when and where the person will report to, can also augment the exploitability of the accused. The clause also provides room for obscurity and secrecy in federal government procedures, allowing the authorities concerned to justify such exploitable laws and procedures, severely infringing upon personal privacy and justified it legally.

Control of subversive associations 10---

> *1. Notwithstanding anything contained in the political parties, act 1962, or in any other law for the time being in force, where the Federal Government is satisfied with respect to any association that there is danger that the association may act in a manner or be used for the purposes prejudicial to the defense or external affairs or the security of Pakistan or of any part thereof, it may, by written or notified order, direct the association to suspend its activities for such period not extending three months as may be specified in the order.*
>
> *2. Where an order under sub-section (1) is in force in respect of an association, any officer authorized by the federal government in this behalf may enter upon and search any premises used for the purposes of the association and take possession of any document belonging to or in the custody of the association in which his opinion may be used for the purpose prejudicial to the defense or external affairs or the security of Pakistan*

Comments

Section 10 of the Act deals in particular with the control of subversive associations and Subsection (1) defines the activities of an organization that are supposed to be subversive if they are prejudicial to defense, external affairs or security of Pakistan. As such, after passing an order, the federal government may suspend its activities for a period not extending three months. Secondly, the federal government may authorize any officer to enter and search any premise allegedly used for said association and take possession of any document therein that is believed to have the possibility of being used for the allegedly criminal purposes.

Here again, the judiciary has been allocated no role in the procedure till the critical stage of violation of the individual or the association's privacy by any person charged by the federal government. This procedural discrepancy, lack of transparency and limitless powers of the investigative officer, augmented with discretional powers to classify documents as prejudicial, leaves a major loophole for exploitation for motives other than the objectives of this Act.

D3 THE PREVENTION OF ANTI-NATIONAL ACTIVITIES ACT, 1974[22]

This Act aims towards the more effective prevention of certain anti-national and treasonable activities of individuals and associations and for matters connected therewith. Our examination of this Act starts with the definition of "anti-national activity" as given in Section 2:

2. Definition

In this Act, unless there is anything repugnant in the subject or context,—

a. "Anti-national activity", in relation to an individual or association means any thing done by such individual or association, whether by committing an act or

(i) Which is intended, or supports any claim, to bring about, on any ground whatsoever, the secession of a part of the territory of Pakistan from the Federation, or which incites any individual or group of individuals to bring about secession;

(ii) Which disclaims, questions, disrupts or is intended to disrupt the sovereignty and territorial integrity of Pakistan;

(iii) Which in any manner encourages or incites, or is intended or is likely or tends to encourage or incite, the public or any group thereof to create, open or continue any regional front or mahaz of any kind based on racial, linguistic or similar ideologies and considerations with a view to disrupting the unity of the people of Pakistan; or

(iv) Which in any manner propagates or advocates that the citizens of Pakistan comprise more than one nationality;

Comments

The definition of anti-national activities as provided by this Act is both broad and vague, particularly in Pakistan's current scenario. The second definition of anti-national activity is of major concern as it marks out any individual or organization as anti-national if s/he/ it disclaims, questions, disrupts or intendeds to disrupt the sovereignty or the territorial integrity of Pakistan.

22. 2011. [ONLINE] Available at: http://www.ma-law.org.pk/pdflaw/THE%20PREVENTION%20OF%20ANTI.pdf. [Accessed 26 May 2011]

With a series of drone attacks in Pakistan and all fingers pointing at the infringement of the sovereignty of the country, one can argue that point two of the definition is obsolete in terms of its scope. This definition of anti-national activities thus places an individual/organization utilizing any communication channel, either print or broadcast, to rightfully disclaim or question the sovereignty of Pakistan at the discretion of the federal government to be listed as anti-national. With the current heightened proclamation of infringed sovereignty on almost all satellite Pakistani channels, we believe this definition must be made void.

CHAPTER II

Anti-national associations

3. Declaration of an association as anti–national

> *1. If the Federal Government is satisfied that any association is, or has become, an anti-national association, it may, by notification in the official Gazette, declare such association to be anti-national.*
>
> *2. Every such notification shall specify the grounds on which it is issued and such other particulars as the Federal Government may consider necessary:*
> *Provided that nothing in this sub-section shall require the Federal Government to disclose any fact which it considers to be against the public interest to disclose.*

Comments

The declaration of being anti-national is subjected to the discretion of the federal government, thus invoking the possibility of political exploitation, as has been a historical trend in Pakistan. Furthermore, the extension of point two of subsection three, i.e. "the federal government may not disclose any fact which it considers to be against public interest to disclose" creates greater room for the victimization of individuals and associations by the State. We would reiterate our position on the need for the supremacy of the judiciary on every matter related to the law and believe that laws that provide the State with discretionary powers to declare people as anti-nationalist, should not be allowed to proceed as they open up countless avenues for political victimization and severe oppression in society. Secondly, the additional power bestowed to the federal government to not disclose any fact that is against public interest to do so, creates room for suspicion: if a person or association is anti-national, there should be no reason to conceal facts from the public so that citizens can be involved in identifying such people/groups to curtail damaging activities.

Article 7: Power to prohibit the use of funds of an anti-national association

> *2. The Federal Government may endorse a copy of an order made under sub-section*
>
> *1. for investigation to any officer of the Government, and such copy shall be a warrant where under such officer may enter in or upon any premises of the person to whom the order is directed, examine the books of such person, search for moneys, securities or credits, and make inquiries from such person or any officer, agent or servant of such person, touching the origin of any dealings in any moneys, securities or credits which the investigation officer may suspect are being used or are intended to be used for the purposes of the anti-national association.*

Comments

Section 2 of ***Article 7*** has a direct association with privacy rights as it allows the federal government to designate any government officer to investigate a matter where the order issued for investigation is to be treated as the warrant for investigation and the assigned officer is given the authority to enter, search and thoroughly investigate the locality, along with the accused person's officer, agent or servant. This section is a continuity of the unlimited power allocated to the federal government to infringe privacy rights by firstly holding a person/organization as anti-national through a notification, without any judicial involvement, and then assigning any government officer, where even the department of that government officer is not explicitly mentioned, the power to thoroughly search and investigate any premises of the accused. The absence of any role of the judiciary throughout the process is of grave concern and acts as a facilitator in the violation of privacy rights.

SECTION E: MISCELLANEOUS LAWS DIRECTLY RELATED TO LAW ENFORCING AGENCIES

E1 CONTROL OF NARCOTIC SUBSTANCES ACT[23]

This Act was promulgated in 1997 and was aimed to consolidate and amend laws relating to narcotics and psychotropic substances, and control the production, processing and trafficking of such drugs and substances. This law has severe implications on the privacy of individuals. Chapter Three of the Act specifically related to "search and investigation" powers and procedures.

CHAPTER III

Search and investigation

20. Power to issue warrant:

1. A Special Court may issue a warrant for the arrest of any person whom it has reason to believe to have committed an offence punishable under this Act, or for the search, whether by day or by night, of any building, place, premises or conveyance in which he has reason to believe any narcotic drug, psychotropic substance or controlled substance in respect of which an offence punishable under this Act has been committed is kept or concealed.

2. The officer to whom a search warrant under sub-section (1) is addressed shall have all the powers of an officer acting under section 21.

Comments

Section 20 gives the officers, on receiving a warrant of arrest for any person from a special court, to search any place at any time of the day with the use of force, if required.

21. Power of entry, search, seizure and arrest without warrant

1. Where an officer, not below the rank of sub-Inspector of police or equivalent authorized in this behalf of the Federal Government or the Provincial Government, who from his personal knowledge or form information controlled substance in respect of which an offence punishable under this Act has been committed is kept or concealed in an building, place, premises or conveyance, and a warrant for arrest or search cannot be obtained against such person without affording him an opportunity for the concealment of evidence or facility for this escape, such officer may:

a) enter into any such building, place, premises or conveyance;

b) break open any door and remove any other obstacle to such entry in case of resistance;

c) seize such narcotic drugs, psychotropic substances and controlled substances and other materials used in the manufacture thereof and any other article which he has reason to believe to be liable to

23. Available at: http://www.fmu.gov.pk/docs/laws/Control%20of%20Narcotic%20Substances%20Act.pd

confiscation under this Act, and any document or other article which he has reason to believe may furnish evidence of the commission of an offence punishable under this Act; and

d) detain, search and, if he thinks proper, arrest any person whom he has reason to believe to have committed an offence punishable under this Act.

2. Before or immediately after taking any action under sub-section (1), the officer referred to in that sub-section shall record the grounds and basis of his information and proposed action and forthwith send a copy thereof to his immediate superior officer.

Comments

Sub-inspectors and higher-grade officers are allowed, through this Act, to perform the operations outlined in Section 20 without obtaining any warrant. This, however, can only be done if the officer concerned has prior information about the presence of the controlled substance and believes that evidence might be concealed or the suspect might escape in the time spent in obtaining a warrant. To make these extraordinary powers of such officers less prone to corruption or misuse, the Act also requires that the officer concerned must record grounds and the basis of his/her information and proposed action and forthwith send a copy thereof to his/her immediate superiors.

CL-E1:

Side Appellant: ARSHAD MAHMOOD
Side Opponent: State

Ss. 20, 21 & 25---Criminal Procedure Code (V of 1898), S.103---Penal Code (XLV of 1860), Ss.441 & 442---Constitution of Pakistan (1973), Art.14---House search and arrest by Magistrate or other agencies in absence of search warrant---Scope---Special provision relating to search and arrest under Control of Narcotic Substances Act 1997 never exempted requirement of search warrant and prior permission for entry into residential premises for purpose of search for same was not inconsistent with the provisions of Cr.P.C. or the Constitution---Purpose of search warrant was to maintain **privacy** of house---Magistrate was neither authorized to enter into premises without due process of law or permission of inmates nor was supposed to exercise his authority of law in any manner he liked---Association of Magistrate in raiding party would be immaterial, where house was raided in disregard to law and in violation of fundamental right of **privacy** ---Public functionaries failing to strictly follow law and observe privacy of house of a citizen could be proceeded against for criminal trespass and damages in their individual capacity---Principles.

23. Power to stop and search conveyance:

An officer referred to in section 19, may, if he has reason to suspect that an conveyance is, or is about to be, used for the transport of any narcotic drug, psychotropic substance or controlled substance in respect of which he suspects that any provision of this Act has been or is being, or is about to be, contravened at any time, stop such conveyance or, in the case of an aircraft, compel it to land and:

a) rummage and search the conveyance or part thereof;

b) examine and search any goods on or in the conveyance; or

c) if it becomes necessary to stop the conveyance, he may use all reasonable force for stopping it.

Comments

Section 23 of the Act authorizes officers mentioned in Section 19 of the Act (there is no officer mentioned in Section 19, which is about forfeiture of assets of an offender; the officer mentioned in ***Article 20***, however, as explained earlier, needs a warrant for search from a special court) to stop and search any conveyance, on land or air, and examine any goods contained therein. But there is no clarity regarding who that officer would be per the provision of this Section: would it a sub-inspector or above or any officer with a warrant from the special court? This blurriness opens gateways for violation of Pakistani citizens' privacy rights.

E2 THE ARMS ACT, 1878[24]

Enacted in 1878, the Arms Act carries a provision in ***Article 25*** that allows a magistrate (within the local limits of his/her jurisdiction), or any officer empowered in his/her behalf, to conduct in his/her presence, the search and seizure of arms from the house or premises of the suspect. This search and seizure operation is subjected to the magistrate first having to record the grounds of his/her belief that arms are present at the point of search.

25. Search and seizure by Magistrate

Whenever any Magistrate has reason to believe that any person residing within the local limits of his jurisdiction has in his possession any arms, ammunition or military stores for any unlawful purpose, or that such person cannot be left in the possession of any such arms, ammunition or military stores without danger to the public peace, such Magistrate, having first recorded the grounds of his belief, may cause a search to be made of the house or premises occupied by such person or in which such Magistrate has reason to believe such arms, ammunition or military stores are or is to be found, and may seize and detain the same, although covered by a license, in safe custody for such time as he thinks necessary.

The search in such case shall be conducted by, or in the presence of, a Magistrate, or by, or in the presence of, some officer specially empowered in this behalf by name or in virtue of his office by the government of Pakistan

E3 PREVENTION OF GAMBLING ACT 1977

This Act promulgated in 1977 aims to curtail gambling in the country and offers rules and procedures for its implementation. Similar ordinances are also present at the provincial tier for all provinces of Pakistan. These ordinances have direct implications for privacy as they allow for entry into and the search of any private place. The power to enter and search, however, is conferred only upon district magistrates and sub-divisional magistrates of the first class and that is subjected to receiving information, performing the necessary inquiry and thus having the reason to believe that the place is used as a gambling den. For entry, they are also provided the authority to use force and are required to allow for female occupants — if they do not appear in public — to withdraw by giving prior notice and reasonable time. The power to seize, take possession of gambling money and equipment, and also of arrest, except for women, is also granted to the officer.

24. 2011. [ONLINE] Available at: http://www.ma-law.org.pk/pdflaw/THE%20ARMS%20ACT.pdf. [Accessed 26 May 2011

Following is the text of the relevant clauses:

8. Power to enter and search

If a District Magistrate, Sub-divisional Magistrate, Magistrate of the first class upon information and after such inquiry as he thinks necessary, has reason to believe that any place is used as a common gaming-house of that an offence under section 6 is being committed at or in any place, he may:

> *a) Enter such place at any time with such assistance as he may require and using such force as may be necessary:*
> *Provided that, if such place is in the actual occupancy of a woman who according to custom, does not appear in public, the officer so entering such place shall give notice to her that she is at liberty to withdraw and, after allowing reasonable time for her to withdraw and giving her reasonable facility for withdrawing, may enter the place;*
>
> *b) Search such place for any instruments of gaming kept or concealed therein, and also the person of all those who are found in that place, except the woman;*
>
> *c) seize and take possession of gaming moneys and securities for money and articles of value reasonably suspected to have been used or intended to be used for the purpose of gaming which are found therein or upon any person found therein; and*
>
> *d) Take into custody all persons, except women found in that place, whether or not then actually gaming.*

CL-E3 | 2010 PLD 21 - QUETTA-HIGH-COURT-BALOCHISTAN

> **Side Appellant:** GHULAM HUSSAIN
> **Side Opponent:** ADDITIONAL SESSIONS JUDGE, DERA ALLAH YAR

Ss. 6 & 8---Constitution of Pakistan (1973) Art.14---Appreciation of evidence---While conducting raid on the house of accused neither Magistrate had inquired into the matter nor was he present when the residence of accused was entered into---Police had no authority to by itself take cognizance of the case under the Balochistan Prevention of Gambling Ordinance, 1978, and its role was only to render assistance to the Magistrate while conducting a raid---Provisions of section 8 of the said Ordinance, thus, had been clearly violated---**privacy** of home could be violated only in certain exceptional circumstances and to do so strict compliance of the applicable law had to be made---Article 14 of the Constitution had also, guaranteed the fundamental right of **privacy** of home---Almighty Allah had himself bestowed such right upon human beings, which had been specifically mentioned in the Holy Quran and in the teachings of Prophet Muhammad, peace and blessings be upon him---Raid having been conducted on the house of the accused in violation of the mandatory provisions of section 8 of the aforesaid Ordinance, any step subsequently taken and any material gathered at the time of raid, was of no consequence and the same could not be relied upon---Accused was acquitted in circumstances.

E4 WEST PAKISTAN REGULATION AND CONTROL OF LOUDSPEAKERS AND SOUND AMPLIFIERS ORDINANCE, 1965[25]

The Ordinance was enacted in 1965, and was further modified by a Bill in 2010, to curtail the spread of sectarianism in particular. The Ordinance carries regulations to safeguard the privacy of individuals in public places as well as residential localities.

Article 2 (1)(a) specifically disallows for the use of a loudspeaker or a sound amplifier in a public or residential locality to cause annoyance or injury to any person thereof. Privacy, as we discussed earlier, is defined as not being disturbed by others and the elements of privacy include solitude. Therefore, this Ordinance protects the privacy of individuals by ensuring that no audio distractions affect his/her personal life or hinders solitude.

Article 2. Restriction on the use of loudspeakers, etc.

> *1. No person shall operate or use or cause to be operated or used a loudspeaker or a sound amplifier:*
> *a) in a public place, in a manner so as to cause or to be likely to cause annoyance or injury to persons residing in any residential locality;*

The penalty for noncompliance with the Ordinance is extended in the Bill of 2010, to increase imprisonment from three months to an year and the fine from Rs 2,000 to Rs 50,000[26].

25. 2011. [ONLINE] Available at: http://www.pakistansocietyofcriminology.com/Admin/laws/TheWestPakistanRegulationandControl.pdf. [Accessed 26 May 2011]

26. Punishment for misusing loudspeaker enhanced to one year in jail | Pakistan Today [ONLINE] Available at: http://www.pakistantoday.com.pk/2011/02/punishment-for-misusing-loudspeaker-enhanced-to-one-year-in-jail/. [Accessed 26 May 2011]

SECTION F: PRIVACY IN THE CYBERSPACE

Industrialization, modernization, globalization and the associated accelerated networking of factors of production across the global village has in turn affected the lives of the people everywhere. The emergence of sophisticated networking has only been made possible as a result of the universal technological quest to support for greater efficacy in our daily lives. Per the estimates of internet world stats, Pakistan had around 18.5 million internet users in June 2009, most of whom are not familiar with the concepts of identity theft or establishing safeguards to protect against various dangers in the cyber world. Online communication and networking has opened new gateways for criminal acts and, therefore, holds strong direct implications on the privacy of individuals.

The increased efficacy of data storage, information processing, and record keeping etc brought about by computers and information technology has elevated the dependence of institutions, offices and individuals in this new paradigm. This has placed at a high amount of risk, the personal information of individuals, their identity, and personal records of people at both private and public institutions.

Pakistan, recognizing the growing involvement of IT in everyday activities, has developed legal documents to curtail any possibilities of electronic crime. Our focus in the following section would be to scrutinize the policy, ordinances and acts promulgated in the country with reference to safeguarding or violating the privacy rights of individuals in the cyber world.

F1 NATIONAL IT POLICY AND ACTION PLAN (2000)[27]

Article 3.4.12.2 under the "IT Policy strategies" section is linked with privacy right and provides recommendations to the IT sector to safeguard the privacy of individuals and the confidentiality of transaction against all possible misuse, excluding even the State, except within the legal framework. The focus of this policy and the action plan regarding privacy is comprehensive as this two-line policy directive (3.4.12.2.4.6) provides a broad policy recommendation to devise detailed laws that protect the privacy of individuals in the cyber domain and provide a safe platform for e-commerce transactions.

3.4.12.2 *IT in the Economy: E-Commerce*

3.4.12.2.4 *Broad policy recommendations for the sector are:*

3.4.12.2.4.6 *To provide safeguards for the privacy of individuals and the confidentiality of transactions against all possible misuse, including that by the State, within the legal framework.*

This document is a guiding framework for the development of privacy laws for cyber domain.

27. 2011. [ONLINE] Available at: http://investinpakistan.pk/pdf/National_IT_Policy.pdf. [Accessed 26 May 2011]

F2 ELECTRONIC TRANSACTION ORDINANCE, 2002

This ordinance referred to as ETO in short was enacted, in 2002, to "recognize and facilitate documents, records, information, communications and transactions in electronic form, and to provide for the accreditation of certification service providers."

The ETO has one article dealing directly with ensuring the privacy rights of individuals in the cyber domain in Pakistan.

36. Violation of privacy of information

Any person who gains or attempts to gain access to any information system with or without intent to acquire the information contained therein or to gain knowledge of such information, whether or not he is aware of the nature or contents of such information, when he is not authorised to gain access, as aforesaid, shall be guilty of an offence under this Ordinance punishable with either description of a term not exceeding seven years, or fine which may extend to one million rupees, or with both.

Comments:

Article 36, under the "Offences" chapter, ensures the privacy of any individual or organization by safeguarding his/her/their information system(s). 'Information system' is defined by the ETO as "an electronic system for creating, generating, sending, receiving, storing, reproducing, displaying, recording or processing information". It is important to mention here that every computer system, whether used at home or at an institution, must fall in this category as every computer system has a strong relationship with information. Therefore, ***Article 36*** guards the information of every person/ information system by placing a punishment of a maximum of seven years in prison, or a fine of Rs1,000,000, or both.

37. Damage to information system, etc.

> *1. Any person who does or attempts to do any act with intent to alter, modify, delete, remove, generate, transmit or store any information through or in any information system knowingly that he is not authorised to do any of the foregoing, shall be guilty of an offence under this Ordinance.*
>
> *2. Any person who does or attempts to do any act with intent to impair the operation of, or prevent or hinder access to, any information contained in any information system, knowingly that he is not authorised to do any of the foregoing, shall be guilty of an offence under this Ordinance.*
>
> *3. The offences under sub-section (1) and (2) of this section will be punishable with either description of a term not exceeding seven years or fine which may extend to one million rupees, or with both.*

Comments

Article 37 further expands the scope of legal protection offered to victims with reference to privacy rights. Subsection (1) clearly states that accessing anyone's private data over any information system, without authorization, is impermissible by law. Subsection (2) comprehensively covers areas of damage to the functioning of information systems that are not directly related to privacy. Both crimes are punishable by either a term not exceeding seven years or a fine which may extend to one million rupees.

Since the lapse of the Prevention of Electronic Crimes Ordinance (PECO) in November 2009, cyber crimes investigations have relied extensively on the ETO for presenting cases in the court of law. PECO is presented next to allow the reader to understand the extent of coverage offered and our analysis on the problems therein, related with privacy rights.

F3 PREVENTION OF ELECTRONIC CRIMES ORDINANCE 2007[28]

PECO 2007 was developed to *"prevent any action directed against the confidentiality, integrity and availability of electronic system, networks and data as well as the misuse of such system, networks and data by providing for the punishment of such actions and to provide mechanism for investigation, prosecution and trial of offences and for matters connected therewith or ancillary thereto."*

Comments

As mentioned above this law has since lapsed. This section has direct relevance to privacy rights in Pakistan. The protection of the confidentiality of electronic systems, networks and data, and devising lawful probations to curtail crimes in that regard is one of the purposes of its establishment. The following section studies the various crimes ordained to be guilty of punishment under this Ordinance with relevance to privacy rights:

CHAPTER II

Offences and Punishments

Chapter two of the ordinance, "Offences and Punishments", deals directly with the various sort of crimes covered.

3. Criminal access.

Whoever intentionally gains unauthorized access to the whole or any part of an electronic system or electronic device with or without infringing security measures shall be punished with imprisonment of either description for a term which may extend to two years, or with fine not exceeding three hundred thousand rupees, or with both.

Comments

Article 3 of Chapter Two deals with criminal access to any electronic system or electronic device. The use of the term "electronic system" or "electronic devise" is all comprehensive and includes a broad spectrum of devises, such as personal computers, servers, and mobile sets etc. This Article has a brief description of the forms in which a person would be regarded as a criminal.

4. Criminal data access

Whoever intentionally causes any electronic system or electronic device to perform any function for the purpose of gaining unauthorized access to any data held in any electronic system or electronic device or on obtaining such

28. 2011. [ONLINE] Available at: http://www.fia.gov.pk/electronic_prevention_orde.pdf. [Accessed 26 May 2011]

unauthorized access shall be punished with imprisonment of either description for a term which may extend to three years, or with fine or with both.

Comments

Article 4 prohibits access to data contained in any electronic system or devise. It imposes a fine, imprisonment or both as punishment.

10. Unauthorized access to code.

Whoever discloses or obtains any password, access as to code, system design or any other means of gaining access to any electronic system or data -with intent to obtain wrongful gain, do reverse engineering or cause wrongful loss to any person or for any other unlawful purpose shall be punished with imprisonment of either description for a term which may extend to three years, or with, or with both.

Comments

Article 10 of Chapter Two places all means of gaining access to any electronic system or data for any unlawful purpose by disclosing or obtaining a password, access to code, system design etc under the crime of unauthorized access to code. There does not seem to be much of a difference between ***Article 3*** and ***4*** and ***Article 10***. The latter seems to be repeating what the prior two articles (3 and 4) have discussed earlier. There seems to be a typographical mistake in the punishment line that does not speak of a punishment that may extend to three years but does not make any description of the extent of fine.

12. Malicious code.

> *1. Whoever willfully writes, offers, makes available, distributes or transmits malicious code through an electronic system or electronic device, with intent to cause harm to any electronic system or resulting in the corruption, destruction, alteration, suppression theft or loss of data commits the offence of malicious code: Provided that the provision of this section shall not apply to the authorized testing, research and development or protection of an electronic system for any lawful purpose.*

Comments

This Article has relevance to privacy as it clearly identifies a person to be committing a crime if s/he commits theft of data through malicious code.

Explanation

For the purpose of this section the expression "malicious code" includes but not limited to a computer program or a hidden function in a program that damages data or compromises the electronic system's performance or uses the electronic system resources without proper authorization with or without attaching its copy to a file and is capable of spreading over electronic system with or without human intervention including virus, worm or Trojan horse.

> *2. Whoever commits the offence specified in sub-section (1) shall be punished with imprisonment of either description for a term which may extend to five years, or with fine or with both.*

14. Spamming

1. Whoever transmits harmful, fraudulent, misleading, illegal or unsolicited electronic messages in bulk to any person without the express permission of the recipient or causes any electronic system to show any such message or involves in falsified online user account registration or falsified domain name registration for commercial purpose commits the offence of spamming.

2. Whoever commits the offence of spamming as described in sub-section (1) shall be punishable with fine not exceeding fifty thousand rupees if he commits this offence of spamming for the first time and for every subsequent commission of offence of spamming he shall be punished with imprisonment of three months or with fine , or with both.

Comments

Article 14 of Chapter Two deals specifically with anti-spamming provisions. Spamming via transfer of harmful, fraudulent, misleading, illegal or unsolicited messages in bulk is considered a crime punishable with a fine not exceeding Rs50,000 for the first time, followed by imprisonment and further fines at later stages. The only point of concern is that 'bulk messaging' is not defined in the Ordinance; there should be some specific quantitative expression describing what bulk is i.e. how many electronic messages in how much time would be regarded as 'bulk'. It also does not take into account the classification of harm done to the recipient on receiving those messages. It has a strong connection with solitude and, therefore, falls under the violation of privacy.

16. Unauthorized interception

1. Whoever without lawful authority intercepts by technical means, transmissions of data to, from or within an electronic system including electromagnetic emissions from an electronics system carrying such data commits the offence of unauthorized interception.

2. Whoever commits the offence of unauthorized interception described in sub-section (1) shall be punished with imprisonment of either description for a term which may extend to five years, or with fine not exceeding five hundred thousand rupees, or with both.

Comments

Article 16 of the Ordinance deals with unauthorized interception of data by technical means. It has a direct relevance to privacy violation and can lead to physical, psychological, monetary and reputational etc harms if left unaddressed.

26. Powers of officer

1. Subject to obtaining search warrant an investigation officer shall be entitled to:

(a) have access to and inspect the operation of any electronic system,

(b) use or cause to be used any such electronic system to search any data contained in or available to such electronic system:

2. The police officer may, subject to the provision, require a service provider to submit subscriber information relating to such services in respect of a person under investigation in that service provider's possession or control necessary for the investigation of the offence:
Provided the investigating officer shall get prior permission to investigate any service provider from the licensing authority where prior permission of the licensing authority is required under any law to investigate the licensed service provider.

3. Any person who obstructs the lawful exercise of the powers under Sub-sections (1) or (2) shall be liable to punishment with imprisonment of either description for a term which may extend to one year, or with fine not exceeding one hundred thousand rupees, or with both.

Comments

Article 26 of the Ordinance entitles investigation officers to search any electronic system after obtaining a search warrant (1). They are also authorized to obtain subscriber information considered necessary for the investigation, from the service provider concerned after obtaining permission from the licensing authority.

27. Real-time collection of traffic data

1. The Federal Government may require a licensed service provider, within its existing or required technical capability, to collect or record through the application of technical means or to cooperate and assist any law enforcement or intelligence agency in the collection or recording of traffic data or data, in real-time, associated with specified communications transmitted by means of an electronic system.

2. The Federal Government may also require the service provider to keep confidential the fact of the execution of any power provided for in this section and any information relating to it.

Comments

The inclusion of ***Article 27*** in the ordinance is an absolute infringement of the essence of privacy right. In simpler terms, it means that the federal government is allowed to look into the online activities of any individual of Pakistan associated with specified communications transmitted by an electronic system. The document fails to mention what those specified communications are. Furthermore, the service provider is required to keep confidential, if deemed necessary by the federal government, the information collected. To curtail the possibility of abuse, it is recommended that the federal government seek permission from the court; that said permission be based upon an objective, neutral, and evidence-based approach that should not be exploitable under any circumstances.

F4 PROPOSED PAKISTAN ELECTRONIC CRIMES ACT (THE "BILL") 2014[29]

The proposed Pakistan Electronic Crimes Bill that is pending before the legislature may also be discussed in this section.

Offences and Punishments

3. Illegal access to information system

1. Whoever intentionally, whether temporary or not,

(a) causes an information system to perform any function with intent to secure access to the whole or any part of any information system or to enable any such access to be secured;

(b) the access he intends to secure or to enable to be secured is unauthorized under this section; and

29. Can be downloaded here: http://www.ispak.pk/Downloads/E-Crime%20Bill%20-Draft%20v%2020.1-clean.pdf

(c) at the time when he causes the information system to perform the function he knows that the access he intends to secure or to enable to be secured is unauthorized under this section shall be punished with imprisonment of either description for a term which may extend to six months or with fine which may extend to one hundred thousand rupees or with both.

Explanation

The absence of authority in this section will also include instances where there may exist general authority to access an information system but a specific type, nature or method of access may not be authorised.

Illustrations

a) A, an employee of B, is authorised by B to generally access and use B's information system at A's place of employment. A is not authorised by B generally, or with respect to any specific type, nature or kind of information to make any copies of, transfer or transmit any information. The employee makes copies of such information, transfers or transmits such information. The act of accessing the information system for the purposeof such copying, transferring, transmitting would amount to access without authority.

b) A, an employee of B, is authorised by B to generally access and use B's information systems at A's place of employment. A is not authorised by B to connect any data storage device to any of B's information systems. A connects a data storage device to B's information system. Such access by A of B's information system is without authority.

2. Whoever recklessly, whether temporarily or not

a) causes an information system to perform any function with intent to secure access to the whole or any part of any information system or to enable any such access to be secured;

b) the access he intends to secure, or to enable to be secured, is unauthorized under this section; and

c) at the time when he causes the information system to perform the function he knows that the access he intends to secure, or to enable to be secured, is unauthorized under this section, shall be punished with imprisonment of either description for a term which may extend to three months or with fine which may extend to fifty thousand rupees, or with both.

Illustrations

a) A, an employee of B is authorised by B to generally access and use B's information system at A's place of employment. A is not authorised by B generally, or with respect to any specific type, nature or kind of information to, make any copies, transfer or transmit any information. The employee whilst browsing the network accesses any part of an information system which he knows he is not authorised to access but does not have a specific intent to access such part of the information system but without such specific intent takes positive steps to access such a part(s) of the information system. Such access would be illegal access with recklessness but not intentional.

b) A, an employee of B is authorised by B to generally access and use B's information systems at A's place of employment. A is not authorised by B to connect any data storage device to any of B's information systems. A connects a data storage device to B's information system. Such access by A of B's information system is without authority.

Comments

This section ensures that information systems including private informations are safeguarded against illegal access. This guards against illegal intrusion into privacy both from outside and within organizations.

5. Illegal interference with program or data

1. Whoever intentionally, whether temporarily or not

(a) does any unauthorised act in relation to an information system;

(b) at the time when he does the act he knows that it is unauthorised; and

(c) acts with intent

(i) to destroy, damage, delete, erase, deteriorate, generate, modify or alter any program or data;

(ii) to render any program or data inaccessible, meaningless, useless or ineffective;

(iii) to obstruct, interrupt or interfere with any program or data or any aspect or attribute related to the program or data;

(iv) to obstruct, interrupt or interfere with any person in the use of any program or data or any aspect or attribute related to the program or data;

(v) to deny, prevent, suppress or hinder access to any program or data to any person entitled to it;

(vi) to deny, prevent, suppress or hinder access to any program or data or any aspect or attribute related to the program or data or make it inaccessible;

(vii) to impair the operation of any program or any aspect or attribute related to the program;

(viii) to impair the reliability of any data or any aspect or attribute related to the data;

(ix) to impair the security of any program or data or any aspect or attribute related to the program or data or

(x) to enable any of the things mentioned in sub clauses (i) to (ix) to be done shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to five hundred thousand rupees, or with both.

These provisions ensure that information systems including private informations are safeguarded against illegal access, guarding against illegal intrusion into privacy both from outside and within organizations. Women and their privacy is especially guarded through the law.

13. Special protection of women

Whoever, with malicious or malignant intent, knowingly transmits any electronic communication that harms the reputation of a woman, threatens any sexual acts against a woman; superimposes a photograph of the face of a woman over any sexually explicit images; distorts the face of a woman; or includes a photograph or a video of a woman in sexually explicit conduct, without the express or implied consent of the woman in question, intending that such electronic communication be exhibited publicly and maliciously intends that such electronic communication cause that woman injury or threaten injury to her good reputation, her existing state of privacy or put her in fear for her safety and such electronic communication in fact has such effect, shall be punished with simple imprisonment for a term which may extend to one year or with fine or with both:

Provided that it shall not be an offence under this section if the electronic communication is an expression of opinion in good faith not done with malicious intent is an expression of criticism, satire or political comment or is analogous to any of the Ten Exceptions under section 499 of the Pakistan Penal Code Act, 1908 (sic):

Provided further that the term "woman" in this section refers to any female regardless of her age who must either be a complainant herself or in the event that she is a minor, her legal guardian must be the complainant While these provisions seem to make intrusions into private information systems inviolable,

While this is a very good clause, the punishment provided under this law is less than the corresponding provision i.e. three (3) years under S. 509 of the Pakistan Penal Code 1860 (It may be pointed out here that the text of the proposed law has a typo since Pakistan Penal Code is from 1860 and not 1908). As special law prevails over general law, this will read out the scope of 509 and its application in cyber space.

The law requires a warrant under Section 19 and Section 20 of the Bill. Subject to the warrant, the investigating officer ("IO") has wide-ranging powers:

21. Powers of an investigating officer

1. Subject to obtaining a search warrant under section 19 An investigation officer shall be entitled to only the information system, program and data specified in the warrant to

(a) have access to and inspect the operation of any specified information system;

(b) use or cause to be used any such specified information system to search any specified data contained in or available to such information system;

(c) obtain and copy that data, use equipment to make copies and obtain an intelligible output from an information system.

(d) have access to or demand any information, code or technology which has the capability of retransforming or unscrambling encrypted data contained or available to such information system into readable and comprehensible format or plain version;

(e) require any person by whom or on whose behalf, the investigating officer has reasonable cause to believe, any information system has been used to grant access to any data within any information system within the control of such person;

(f) require any person having charge of or otherwise concerned with the operation of such information system to provide him reasonable technical and other assistance as the investigating officer may require for the purposes of clauses (a), (b) and (c); and

(g) require any person who is in possession of decryption information of an information system, device or data under investigation to grant him access to such decryption information necessary to decrypt data required for the purpose of investigating any such offence:
Provided that this power shall not empower an investigating officer to compel a suspect or an accused to provide decryption information, or to incriminate himself or provide or procure information or evidence or be a witness against himself.

Explanation

Decryption information means information or technology that enables a person to readily retransform or unscramble encrypted data from its unreadable form and from cipher text to its plain text.

While the law has been drafted to incorporate many of the 13 Principles, especially in sub-section (2) of the section above read with section 23 of the Bill, which have not been reproduced here, including but not limited to proportionality, a proper judicial forum, user notification and strictly on a necessity basis, but given the prevailing situation in Pakistan vis a vis abuse of authority and law and order, this is likely to be misused. The law impacts the cyber space in the following ways:

- a person accessing an information system – any device that has processing power, operates electronically and stores sensitive and private data – without authorization may face imprisonment for up to six months and a fine of up to Rs. 100,000 or both. Changing content of information system may result into imprisonment of up to nine months or a fine of up to Rs. 200,000.

- Unauthorized destruction/deletion of data may result into imprisonment of up to three years or a fine of up to Rs. 500,000 or both.

- Accessing an information system to spread panic/fear or if such access is rated as severe cyber terrorism then punishment can extent to imprisonment for up to fourteen years or a fine of up to Rs. 50 million or both.

- Electronic forgery will be punished with imprisonment of up to two years or a fine of up to Rs. 200,000 or both.

- If electronic fraud is found and proved then guilty can face an imprisonment of up to five years or a fine of up to Rs. 10 million or both.

- If someone is found guilty of posing another person's identity then he/she may face imprisonment of three months of a fine of Rs. 50,000 or both.

As mentioned above the law also introduces the following punishments against infringement of private data.

- Unauthorized interception of private data (for example hacking emails) can result into imprisonment of two years or a fine up to Rs. 500,000 or both.

- Special protection for women: If someone is found publicly spreading any content (video/pictures/audio) that may harm the reputation of women then he/she may face imprisonment for one year or a fine up to Rs. 1 million or both.

The real question however is the state's power to infringe on the privacy. In this respect the following section is especially disturbing:

30. Real time collection and recording of data.

1. If a Court is satisfied on the basis of information on oath on an application by an investigating officer that there are reasonable grounds to believe that the content of any specifically identified electronic communications is reasonably required for the purposes of a specific criminal investigation, the Court may

order with respect to traffic data held by or content data having passed through a service provider within its jurisdiction, through application of technical means, to

(a) have that service provider collect or record traffic data in real time; and

(b) and where administratively and financially not burdensome and technically possible collect or record content data in real time, conducted only through and in coordination with and facilitated by the intelligence agency or intelligence service referred to in s ection 50 of this Act and specially notified for the purposes and in respect of this section by the Federal Government associated with only the specified communications and related to or connected with only the person under investigation transmitted by means of an information system and provide only the specified traffic data and where applicable content data, to the investigating officer
Provided that such real time collection or recording shall not be ordered for a period beyond what is absolutely necessary and in any event not for more than seven days.

2. The period of real time collection or recording may be extended beyond seven days if, on an application, the Court authorizes an extension for a further specified period of time
Provided that any extensions will require a full rehearing of the matter and the standard for satisfaction of the Court shall be higher with every application for extension.

3. The Court may also require the service provider to keep confidential the fact of the execution of any power provided for in this section and any information relating to it.

4. The application under sub sections (1) and (2) shall in addition to substantive grounds and reasons also

a) explain why it is believed the traffic data and where applicable content data sought will be available with the person in control of the information system;

b) identify and explain with specificity the type of traffic data and where applicable content data suspected will be found on such information system;

c) identify and explain with specificity the identified offence made out under this Act in respect of which the warrant is sought;

The problem again is that while there is a palpable attempt to meet the 13 Principles, there is a clear absence of user notification and public oversight. Furthermore the problem in Pakistan is not as much the word of the law but how that law is practically implemented on ground and conditions in Pakistan suggest that this law will prove to be an impediment to privacy instead of protecting and safeguarding it.

F5 INVESTIGATION FOR FAIR TRIAL ACT, 2013[30]

The Investigation for Fair Trial Act (for the purposes of this section the "Act"), passed by the National Assembly on 20 December 2012 and by the Senate on 24 January 2013 is a draconian infringement on the fundamental right to privacy and human dignity of an individual and as such violates many of the 13 Principles.

First and foremost, one must recognize that any surveillance, given Pakistan's chequered history, may or may not have a legitimate aim. While one must recognize that surveillance and tapping are undertaken even by the most democratic of countries, it may be stated that in Pakistan's particular context, the Act is likely to empower those elements who may use the material with impunity to blackmail and strong arm dissenting voices, civil society activists and sectarian minorities.

30. Available at: http://www.na.gov.pk/uploads/documents/1361943916_947.pdf

The Act provides for the following:

- A procedure to sanctify state surveillance of citizens with impunity- hence is in violation of the requirements of necessity, legitimate aim, adequacy and proportionality as envisaged by the 13 Principles. It goes without saying that actions taken under the Act are unlikely to be proportional and necessary.

- Clothes the procedure in respectability by making the Judge of the High Court the keeper of conscience but this is more for show. In any event, the requirement of the 13 Principles is of determination by an impartial body both before and after the fact, while the Act does not necessarily lay down any requirements for post-hoc determination of the materials collected through surveillance. It also brings the provisions of the Act in direct conflict with the transparency requirements of the 13 Principles.

- Clothes intelligence agencies with the power to monitor and intrude in the private space of the citizen, through secret court orders, and such violates the requirements for public oversight, user notification and due process under the 13 Principles.

- The Act essentially allows the functionary of the state to obtain a warrant in secret if, inter alia, the applicant body "has reasons to believe" that any citizen or any other person "likely to be associated" with or is "beginning to get associated with" or is in the "process of beginning to plan" or "likely to plan or attempt" a scheduled offence. Instead of following the probable cause standard, the law makers have made "reasons to believe" the standard.

- The requirement for user notification as well as competent judicial authority is sidestepped. Consider for example that warrant is to be issued by a High Court judge without any notice to the subject of such an order i.e. the subject and cover everything including audio, video, text messages, emails. Thus the Act, when read with the Anti Terrorism Act 1997 as amended by the Anti Terrorism Ordinance ("Ordinance"), is a catchall for all forms of surveillance that are imaginable.

- The idea behind the Act is to provide a basis for complete and total control for 60 days and on the basis of mere suspicion. This is neither reasonable nor constitutional. The idea is to seek prevention of a crime before it is actually committed. All of these amount to gross violation of the aforesaid 13 Principles, including but not limited to proportionality, transparency, and safeguards with respect to illegitimate access.

- It must not be forgotten that for the population at large, such intrusions count as a serious loss of civil liberties and have been widely criticised in the developed world too. In giving state agencies wide-ranging powers to monitor citizens' private lives and conversations, the possibilities of misuse and abuse are immense. Further, Pakistan must be delineated from countries such as the US or UK because of its history of intelligence agencies' involvement in manipulating political outcomes. To what extent should monitoring powers mentioned in the proposed bill be granted, and to which agencies, should be worth pondering.

There are no two opinions that legitimate cases of terrorism and anti-national activities may be monitored legitimately, but the Act provides no safeguards whatsoever against misuse of the law to persecute people by the state authorities. The law requires a mere affidavit as supporting evidence for an application for surveillance made under Section 8 of the Act. Section 8 (c) i reads:

> c. The application for the issuance of warrant shall be accompanied by:
> i) A signed statement and affidavit of the authorized officer that the contents of the report and application are true and correct to the best of his information and that the warrant shall be used only and exclusively for preventing or lawfully investigating a scheduled offence or to collect evidence in respect thereof and the same shall neither be misused in any manner nor shall the approval of the warrant be abused to interfere or intervene in the privacy of any person.

Section 10 plays lip service to privacy when it states the following:

> 2. The Judge while passing an order for the issuance of warrant shall ensure that:
> a) the authorized officer is properly authorized to represent the applicant; and
> b) the issuance of warrant shall not unduly interfere in the privacy of any person or property.

Officials may ask for a warrant if they believe a person is going to commit or plan a scheduled offence and will need to prepare a report. This report will be approved by the department's head or a BPS-20 officer and then submitted to a judge. The offences that are included here are from a number of laws, including the Official Secrets Act and the Anti-Terrorism Act. This means that if the government believes someone is leaking official secrets, they can ask for the suspect's e-mail and phones to be tapped, and similarly, if it suspects that someone is planning a terrorist attack or making extortion demands. Currently, the police get access to data after making requests to the Inter-Services Intelligence. The warrant – which can extend for up to six months – will be issued by the judge in his/her chambers and will not be a public record. Who will provide this data? The data will be given by 'service providers', such as telecom operators or internet service providers. They will have indemnity, which means citizens can't sue them for handing over their data. A service provider who declines to provide information can be fined up to Rs10 million or jailed for two years.

What data can the government access? According to the law, the government can access "data, information or material in any documented form … through audio visual device, CCTV, still photography, bugging, observation or any mode of modern devices or techniques obtained under the Act … documents, papers, pamphlets, booklets" for surveillance. The government can also intercept emails, SMS, internet protocol detail record, call detail record and any form of computer based or cell phone based communication. It also includes any means of communication using wired/wireless/internet protocol-based media/gadgetry. Thus the integrity of communications systems becomes suspect and vulnerable. How this will be balanced out against the requirements under the proposed cyber crimes law remains to be seen as the latter legislation is still in the works.

The Act does not provide the following which are otherwise required by the 13 Principles:

- Specific instances initiating surveillance. Mere suspicion – which may well be a question of personal likes and dislikes and/or vendetta- backed by an affidavit is proof enough to initiate surveillance. Thus necessity, proportionality and legitimate aim are to be the casualties of this exercise.

- Surveillance as the method of last resort i.e. after systematically showing that all other conceivable ways of determining the guilt or lack thereof of an individual have been exhausted.

- Critically the Act does not provide any real and meaningful provision for capacity building for institutions, especially constitutional and other legal sensitivities. No discussion is available to limit the possibility of abuse. Finally and most conspicuously there is no competent judicial forum to oversee the determinations pertaining to the data that has been collected.

While there is some real attempt to at least appear to make it look as if the process is not entirely arbitrary, especially since the judicial officer envisaged under the Act is a Judge of the High Court, not enough protection or safeguards are granted for the would be/suspected future offender to give him or her the benefit of doubt and the opportunity to be heard. Again while it purports to have judicial oversight of the warrant, it foresees no role for judicial oversight of the data thus collected.

The arbitrary nature of the violations these statutes amount to in terms of privacy obligations is further cemented by the ratios of some of the more celebrated decisions of the Supreme Court:

In **Jamat-i-Islami Pakistan v. Federation of Pakistan (PLD 2000 SC 111)**:

"It is well-settled that Statutes must be intelligibly expressed and reasonably definite and certain. An act of the Legislature to have the force and effect of law must be intelligibly express and statutes which are too vague to be intelligible are a nullity. Certainty being one of the prime requirements of a statute, a statute in order to be valid must be definite and certain. **Anticipated difficulty in application of its provisions affords no reason for declaring a statute invalid where it is not uncertain. Reasonable definiteness and certainty is required in statues and reasonable certainty is sufficient.** Reasonable precision, and not absolute precision or meticulous or mathematical exactitude, is required in the drafting of statutes, particularly as regards those dealing with social and economic problems."

In Pakistan Tobacco Co. Ltd. vs. Government of NWFP (PLD 2002 SC 460), the Supreme Court of Pakistan held:

"There is consensus of the judicial opinion that delegation of powers should not be **uncontrolled, unbridled and to check the arbitrary attitude of the Executive in exercise of powers the legislature must provide some guidelines basing on the policy of the government to exercise such powers**."

It is settled law that penal provisions must explicitly define the conduct of a criminal and unless it clearly and categorically defines its boundaries, it would be treated as an arbitrary enactment, because the citizens against whom a penal action is proposed, has no notice that on account of what type of conduct he is being charged and has been held responsible for penal consequences.

The Supreme Court has repeatedly held legislations like the Act, which give unbridled, unguided discretion to executive functionaries to be unconstitutional. The ratio of **Waris Meah v. State (PLD 1975 SC 157)** serves the purpose:

"Here, not only is there discretion in the specified authorities whether they will proceed at all against any member of the class concerned, viz. offenders against the Act, but there is also an unfettered choice to pursue

the offence in any one of three different modes which vary greatly in relation to the opportunity allowed to the alleged offender to clear himself, as well as to the quantum and nature of the penalty which he may incur. The scope of the unguided discretion so allowed is too great to permit of application of the principle that equality is not infringed by the mere conferment of unguided power, but only by its arbitrary exercise. For in the absence of any discernible principle guiding the choice of forum, among the three provided by the law, the choice must always be, in the judicial view point, arbitrary to a greater or less degree. The Act, as it is framed, makes provision for discrimination between persons falling, qua its terms, in the same class, and it does so in such manner as to render it impossible for the Courts to determine, in a particular case, whether it is being applied with strict regard to the requirements of ***Article 5*** (1) of the Constitution."

In **Mehram Ali v. Federation of Pakistan (PLD 1998 SC 1445)**, we saw the Supreme Court similarly rising to the occasion and striking down a provision of the Anti-Terrorist Act in the following terms:

"The conferment of power on the officers referred to in clause (i) of subsection (2) of section 5 without being fired upon by the accused is not justifiable. An officer of any of the above forces under the present provision can kill any person, if he considers that in all probability the former is likely to commit a terrorist act or scheduled offence. The formation of opinion as to the probability or likelihood of commission of offence will vary from person to person as it depends on subjective satisfaction. There is no check or guideline provided for the exercise of the above power conferred by the above provision. We are, therefore, of the view that the aforesaid provision in its present form is not sustainable. The same may be amended and it may be provided that the officer can fire upon an accused person if he has been himself fired upon by him."

SECTION G: SECTOR SPECIFIC LAWS

G1 PAKISTAN MEDICAL & DENTAL COUNCIL CODE OF ETHICS[31]

The records held by medical authorities are the private property of the patient. The patient-physician relationship is therefore considered a vital bond of confidentiality to safeguard the patient against many unwanted outcomes that can have an adverse effect on her/his reputation, personal relationships, social bonds and lawful obligations etc. This bond is therefore based on a high level of trust, which must be protected, and for which the Pakistan Medical & Dental Council has developed a Code of Ethics.

Section 5 of the PM&DC code of ethics is regarding the oath of medical and dental practitioners. This oath expresses the confidence and trust that the patient should have while discussing his/her medical condition with the doctor as the information is not to be disclosed even after the patient has died.

Section 5: Oath of medical and dental practitioners

- *I will respect the secrets which are confided in me, even after the patient has died;*
- *The Article 10 of the code again points to the right to privacy/confidentiality in an explicit mannner.*

10.0. Fundamental Elements of Patient – Physician Relationship

10.4 The patient has the right to confidentiality

12.0. Confidentiality

The physician has a right to and should withhold disclosure of information received in a confidential context, whether this be from a patient, or as a result of being involved in the management of the patient, or the review of a paper, except in certain specific circumstances where s/he may carefully and selectively disclose information where health, safety and life of other individual/s may be involved.

12.1 - The practitioner cannot seek to gain from information received in a confidential context (such as a paper sent for review) until that information is publicly available.

12.2 - There is no legal compulsion on a doctor to provide information concerning a criminal abortion, venereal disease, attempted suicide, or concealed birth regarding his patients to any other individual or organization. When in doubt concerning matters, which have a legal implication, the practitioner may consult his/her legal adviser

12.3 - The professional medical record of a patient should not be handed over to any person without the consent of the patient or his/her legal representative. Generally speaking, the state has no right to demand information from the doctor about his patient, save when some notification is required by statute such as in the case of communicable diseases. When in doubt, a legal advisor should be consulted.

31. 2011. [ONLINE] Available at: http://www.pmdc.org.pk/Ethics/tabid/101/Default.aspx. [Accessed 26 May 2011]

12.4 - A presiding judge, may, despite the physician claiming the knowledge and communication is confidential overrule this contention and order or direct the witness to supply the required information. The doctor has no option but to comply unless willing to accept imprisonment for contempt of court.

Comments

Article 12 deals extensively with confidentiality of information and starts with extending the means by which information can be received by the physician. It disallows the practitioner from seeking information received in a confidential context (12.1), does not place any legal obligation on the doctor to provide information to any person or organization on any medical case (12.2), excludes the governmental right to take the professional medical record of patients without their prior consent (12.3), but it allows the presiding judge to obtain any information from the physician, the compliance of which is obligatory and the refusal to do so is considered contempt of court.

G2 BANKING COMPANIES RULES 1963[32]

This Ordinance also provides safeguards for financial information, which is one of the most critical aspects of a person's privacy. There are only two situations in which the SBP is allowed to publish information: when it is in public interest to do so or at the time of holding of elections of persons on whom payments of loans, advances and credits have been due for more than an year. The second situation requires that a prior notice be given to such a person and the opportunity of hearing be provided.

Article 33. Power to publish information

The State Bank, if it considers it in the public interest so to do, may publish any information obtained by it under this Ordinance in such consolidated form as it thinks fit.

CL-G2 | 2010 LAHORE-HIGH COURT

Side Appellant: M.D. TAHIR, ADVOCATE
Side Opponent: DIRECTOR, STATE BANK OF PAKISTAN

Seeking personal and financial information of individual citizen's accounts by Banks and other financial institutions. The State Bank of Pakistan issued a directive requiring Banks/Financial Institutions to supply to Central Board of Revenue information regarding profit/return in excess of Rs. 10,000 paid to account-holders/depositors along with their names, addresses, National Tax Numbers and National Identity Card Numbers.

The Lahore High Court held that taking private information without any allegation of wrong doing of ordinary people would affect their life, making them potentially vulnerable and insecure, and that it represented an extraordinary invasion of their fundamental right of privacy. Such direction in the nature of subordinate legislation was illegal, bad on the grounds of unreasonableness, discriminatory being ultra vires of ***Articles 4*** & ***25*** of the Constitution. The High Court accepted a Constitutional petition and struck down the impugned Circular as being without lawful authority.

32. 2011. [ONLINE] Available at: http://www.sbp.org.pk/publications/prudential/ordinance_62.pdf. [Accessed 26 May 2011]

Article 33A. Fidelity and secrecy

1. Subject to sub-section (4.), every bank and financial institution shall, except as otherwise required by law, observe the practices and usage customary among bankers and, in particular, shall not divulge any information relating to the affairs of its customers except in circumstances in which it is, in accordance with law, practice and usage customary among bankers, necessary or appropriate for a bank to divulge such information.

2. Every president, chairman, member of the Board, administrator, auditor, adviser, officer or other employee of any bank and financial institution shall, before entering upon his office, make a declaration of fidelity and secrecy in such form as may be prescribed.

4. The State Bank of Pakistan may, if satisfied that it is necessary so to do at the time of holding general elections under any law relating thereto, publish a list of persons to whom any loans, advances or credits were extended by a bank or financial institution, either in their own names or in the names of their spouses or dependents or of their business concerns (if mainly owned and managed by them) which were due and payable and had not been paid back for more than one year from the due date, or whose loans were unjustifiably written off in violation of banking practices, rules or regulations on or after such date as may be determined by the Government:
Provided that before publishing the name of any person in any such list he shall be given prior notice and, if he so requests, an opportunity of hearing.

G3 PRESS COUNCIL OF PAKISTAN ORDINANCE, 2002[33]

The Press Council of Pakistan Ordinance 2002 places a thorough set of obligations upon the press, under the supervision of a press council, whose function it is to develop, enforce and implement the ethical code of practice to oblige with a wide array of regulations that explicitly address the rights of personal privacy.

8. Functions of the Council

1. The Council shall perform the following functions, namely:

(iv) To revise, update, enforce and implement the Ethical Code of Practice for the newspapers, news agencies, editors, journalists and publishers as laid down in the Schedule to this Ordinance;

(v) To receive complaints about the violation of Ethical Code of Practice relating to newspapers, news agencies editors and journalists;

(vi) to appoint Enquiry Commissions to decide complaints at the head office, all provincial sub-offices and regions, as the case may be necessary for its proper functioning;

The ethical code of practice is given hereunder:

Ethical Code of Practice:

1. The press shall strive to uphold standards of morality and must avoid plagiarism and publication of slanderous a libelous material.

33. 2011. [ONLINE] Available at: http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/3.%20Pakistan%20Press%20Council%20Ordinance%202002.pdf. [Accessed 26 May 2011].

4. The Press shall respect the privacy of individuals and shall do nothing which tantamounts to an intrusion into private, family life and home.

7. The Press shall avoid originating, printing, publishing and disseminating any material, which encourages or incites discrimination or hatred on grounds of race, religion, caste, sect, nationality, ethnicity, gender, disability, illness, or age, of an individual or group.

14. In the case of sexual offences and heinous crime against children, juveniles and women, names and identifying photographs shall not be published.

15. Confidentiality agreed upon at briefings and background interviews must be observed.

Comments

The schedule of the Ordinance identifies the ethical code of practice as referred to earlier. The ethical code of practice has five articles that guarantee the right of privacy to individuals. ***Article 1*** focuses on curtailing the publication of slanderous and libelous material, ***Article 4*** disallows for intrusion into the privacy of the private sphere, family and home. ***Article 7*** aims to curb discrimination and hatred towards any group or individual on a broad spectrum of aspects. ***Article 14*** safeguards the privacy of women and children that are victims of sexual offenses and crimes by curtailing the publication of their names and photographs. And lastly, ***Article 15*** requires that confidentiality be agreed upon during briefings and background interviews.

G4 PAKISTAN TELECOMMUNICATION (RE-ORGANIZATION) ACT 1996[34]

This Act aims to provide for the reorganization of telecommunication system in Pakistan by establishing the Pakistan Telecommunication Authority, the Frequency Allocation Board, National Telecommunication Corporation and the Pakistan Telecommunication Employees Trust; the regulation of the telecommunication industry; the transfer of telecommunication services to the private sector; and for matters connected therewith or incidental thereto.

32. Warrants for search

1. Where on information furnished by the Authority or Board, the Court has reason to believe that any unlicensed telecommunication system, wireless telegraphy apparatus or unapproved terminal equipment is being kept or concealed or any unlicensed telecommunication service is provided, it may issue a search warrant; and the person to whom such warrant is directed, may enter the premises, vessel, aircraft, or hovercraft where such telecommunication system, wireless telegraphy apparatus or terminal equipment is allegedly kept or concealed or unlicensed telecommunication service is provided there from carry out search and inspection thereof and seize such telecommunication system, wireless telegraph apparatus or terminal equipment.

Comments

Article 32 of the Act allows the authority (Pakistan Telecom Authority) or the board (Frequency Allocation Board, one of whose functions it is to instigate all complaints of interference and take appropriate action to effect clearance) to submit information regarding illegalities to the court. The court may issue a search warrant of the premises used for the crime, carry out investigation and seize the equipment used.

34. 2011. [ONLINE] Available at: http://www.privatisation.gov.pk/PDF-Files/Telecon%20Act.PDF. [Accessed 26 May 2011]

The involvement of the court in the process, unlike most other laws in the country, portrays a pragmatic attitude towards ensuring that rights in general and privacy rights in particular are not exploited and an element of accountability is displayed. As we see in ***Article 54*** of the Act, i.e. National Security, however, the federal government has separated its unlimited powers to intercept calls in the interest of national security or in the apprehension of an offense.

33. Indemnity

No suit, prosecution or other legal proceedings shall lie against the Authority or any member or employee of the Authority in respect of anything done or intended to be done by the Authority in good faith under this Act.

Comments

Article 33 disallows any suit, prosecution or legal proceeding to be taken against Authority or a member/employee of authority for actions done in good faith. The only point of concern here is that "good faith" can never be defined as it is a qualitative, intangible element. This allows for greater political and institutional exploitation while opening avenues for avenging personal disputes: a member of the board could, in theory, submit a false report in "good faith" and destroy both the privacy and the reputation of the accused and remain unaccountable as 'good faith' cannot be challenged.

A justified and logically-constructed complaint procedure must therefore be enacted to replace subjective initiations. A consultative mechanism with proper documentation must be presented to the court as copies of evidence, signed by senior authorities so as to curtail any possibility of the violation of privacy rights.

58. Ordinance to override other laws

The provisions of this Act shall have effect notwithstanding anything contained in the Telegraph Act, 1885 (XIII of 1885), the Wireless Telegraphy Act, 1933 (XVII of 1933), or any other law containing any provision inconsistent to this Act.

Miscellaneous

54. National Security

> *1. Notwithstanding anything contained in any law for the time being in force, in the interest of national security or in the apprehension of any offence, the Federal Government may authorize any person or persons to intercept calls and messages or to trace calls through any telecommunication system.*

Comments

Article 54 of the miscellaneous section is the most questionable. This is the controversial listening in provision. Here again, the federal government has bestowed itself with unlimited powers to allow any person to intercept any call or message or to trace calls through any telecommunication system in the interest of national security or for the apprehension of an offense. Although this Article has been categorized under the miscellaneous section, it has the most severe implications on privacy, for two main reasons. Firstly, as discussed earlier, even in matters of national security, the court must be given precedence in deciding where such intrusion is

permissible. Secondly, the federal government has increased its powers manifold to include the second causality of "apprehension of any offense". The category of offense that is subjected to such procedure is not mentioned and the time for which the suspect would be monitored is not explicitly mentioned. The federal government has a right to monitor, for example, the private calls of a man to his wife for days, months or years on the "apprehension" that this person might steal books from a library. Such laws are an impediment to the realization of the nation's potential and they allow a democratically-elected federal government to exercise powers far greater than the colonial masters for violating basic human rights that are critical for societal progress. In terms of the 13 Principles, it violates the requirement of a competent judicial forum, public oversight and user notification, none of which is available under the law as it is currently worded. It is used as a catch all by the government as it affects all forms of telecommunications based interaction.

G5 TELECOMMUNICATION RULES 2000[35]

The PTA Telecommunication Rules of 2000 is a document governing the relationship between the authority (PTA) and the licensee. The document is comprehensive and elaborates the codes and procedures that need to be followed while granting licenses and associated services. These rules are important for our discussion as telecommunication governs the lives of almost a million people across Pakistan.

These rules provide consumers with privacy protection over telecommunication networks. The articles related to privacy are briefly discussed below:

Part 11 of the general license conditions, "conditions", places an obligation on every licensee to abide by Schedule 2 annexed with the document. The condition clause states:

11. Conditions:

The license and licenses Services shall be subject to the conditions as specified in the Schedule 2 annexed hereto:

The schedule two carries amongst other conditions, a "code of practice for consumer affairs". The licensee, in consultation with the Authority, is required to prepare and publish within six months after the Effective Date, a Code of Practice to govern its dealings with customers. The code of practice contains six requirements amongst which article "d" is of importance with relevance to privacy. It states:

The Code of Practice shall include, at a minimum, provisions covering the following issues, namely:

d) Protection and preservation of privacy of information transmitted over the public switched network;

***Section 4** of "Conditions" is related to the "confidentiality of customer information". It requires the licensee to prepare a "confidentiality code", in consultation with the PTA, and places the obligation upon the employees of the licensee to abide by it. The licensee is required to give the PTA in writing that all steps have been taken to ensure that all employees who have access to or might have access to the personal information of customers are abiding by the confidentiality code. The text of **Section 4** our is given below:*

35. 2011. [ONLINE] Available at: http://www.pta.gov.pk/media/rules_280208.pdf. [Accessed 26 May 2011]

4. Confidentiality of Customer Information

4.1 - The Licensee shall take all reasonable steps to ensure that those of its employees who obtain, in the course of their employment, information about customers of the Licensee or about the customer's business ("Customer Information") observe the provisions of a code of practice on the Confidentiality of Customer Information (the "Confidentiality Code").

4.2 - The Confidentiality Code shall be prepared by the Licensee in consultation with the Authority and shall:

(a) Specify the persons to whom Customer Information may not be disclosed without the prior consent of that customer; and

(b) Regulate the Customer Information which may be disclosed without prior consent of that customer.

4.3 - The Licensee shall, within three months of the date on which the provisions of the Confidentiality Code have been agreed with the Authority, confirm in writing to the Authority that it has taken all reasonable steps to ensure that those of its employees who obtain or are likely to obtain Customer Information are observing the provisions of the Confidentiality Code.

4.4 - This Condition 14 shall apply without prejudice to any duties of the Licensee towards its customers under the law.

Comments

Article 4.2(a) is of serious concern here as Section "a" says that the code shall specify the persons to whom customer information may not be disclosed without the prior consent of the customer. The first thing that pops up in mind is that there will be persons to whom the customer information will be disclosed without the prior consent of the customer, and those are not mentioned in the list. The clause could have been more straightforward if the list of the persons or departments allowed to obtain customer information without their consent would have been given instead of the other way around.

54. National Security

1. Notwithstanding anything contained in any law for the time being in force, in the interest of national security or in the apprehension of any offence, the Federal Government may authorize any person or persons to intercept calls and messages or to trace calls through any telecommunication system.

Comments

Article 54 explicitly states that the federal government has a right to infringe upon individual privacy in matters of national security or in the "apprehension of any offence". National security is a broad term that in itself has an extensive applicability, whose interpretation can be directed to a large number of activities. More distressing is the addition of the exception of "any offence" in telecommunication rules. No explanation or classifications has been provided for "any offence" in the rules. We consider it a big loophole in the provision of adequate privacy to individuals in Pakistan. We believe that the offences that could trigger interceptions should either be exhaustively mentioned, or references be given in association with other laws of the country (the PPC, for example). Secondly, instead of authorizing any person, the government should mention who those persons would be and the department to which they would belong. Thirdly, interception should be subject to orders obtainable through a court. This is critical to ensure that ***Article 54*** is not exploited for motives other than explicitly mentioned.

CL-C2 | Case law: PLD 1998 SC388 SUPREME COURT

Petitioners: MOHTARMA BENAZIR BHUTTO AND OTHERS
Respondants: PRESIDENT OF PAKISTAN AND OTHERS

Dissolution of National Assembly and dismissal of Prime Minister and the Cabinet by the President under Art.58(2)(b) of the Constitution---Grounds---Validity---Link was established between the Prime Minister and the illegal and unconstitutional act of tapping phones and eavesdropping of citizens, Judges of the superior Courts, leaders of political parties and high ranking military and civil officers---Tapping or eavesdropping of citizens to whatever class, group or status they may belong, was not only an offence under Telegraph Act but it also offended against Arts. 9 & 14 of the Constitution of Pakistan---Such ground alone, held, was sufficient to dissolve the National Assembly by the President under Art.58(2)(b) of the Constitution.

Telephone tapping and eavesdroppings mar the protection afforded and guaranteed to the right to life and infringe the secrecy and privacy of a man---"Privacy of home"---Connotation---Telephone tapping and eavesdroppings being unconstitutional, appropriate mode of its regulation was desired by the Supreme Court---Supreme Court, however, observed that so long proper law was not legislated in the field which may protect the violation of Constitutional rights, in future whenever any telephone is required to be tapped, intruded or eavesdropping exercise is to be carried on, it should be done with the prior permission of the Supreme Court or by a Commission constituted by the Supreme Court which shall examine each case on its merits---Permission if granted by the Supreme Court or the Commission as the case may be, shall not exceed a period of six weeks and shall be reviewed immediately on expiry of six weeks.

G6 THE TELEGRAPH ACT 1885[36]

This Act came into force on October 1, 1885. Telegraph is defined under Subsection (1) of ***Section 3***:

3. Definitions

In this Act, unless there is something repugnant in the subject or Context:

> *1. 'telegraph' means any apparatus, equipment or plant used for transmitting, emitting, making or receiving signs, signals, writing, speech, sound or intelligence of any nature by wire, radio or visual or electromagnetic system.*

5. Power for Government to take possession of licensed telegraphs and to order interception of Messages

> *1. On the occurrence of any public emergency, or, in .the interest of the public safety, the Federal Government or a Provincial Government or any officer specially authorised in this behalf by the Federal Government or a Provincial Government, may:*
>
> *(a) Take temporary possession of any telegraph established, maintained or worked by any person licensed under this Act: or*

36. 2011. [ONLINE] Available at: http://www.pakistansocietyofcriminology.com/Admin/laws/TelegraphAct1885.pdf. [Accessed 26 May 2011]

(b) Order that any message or class of messages to or from any person or class of persons or relating to any particular subject brought for transmission by or transmitted or received by, any telegraph, shall not be transmitted, or shall be intercepted or detained, or shall be disclosed to the Government making the order or any officer thereof mentioned in the order.

(2) If any doubt arises as to the existence of a public emergency, or whether any act done under subsection (1) was in the interest of the public safety, a certificate of the Federal Government or, as the case may be, the Provincial Government shall be conclusive proof on the point.

Comments

Article 5 defines the powers of the federal or provincial government to take temporary possession of any telegraph established, maintained or worked by any person licensed under this act (a) or order for the interception, detention or disclosure of any class of message by any person/class of persons to the government. The reason for both these sub-articles (1) and (2) are public emergency or public safety. Furthermore, any doubts regarding the validity of such actions shall be dealt with by a certificate of the federal or the provincial government justifying its actions.

Similar to most other acts where the State is bestowed with absolute authority without any involvement of the judiciary, this Act also allows the government, both federal and provincial, to intervene, disrupt and take away the privacy of communication from people and leaves no room for any accountability of the state in any court of law.

Although telegraphic communications have become obsolete with the advent of modern technologies, these outdated laws, propagated in the Colonial Era, are kept intact to disallow for any domain left from the interruption of government, and to ensure that the powers of the State remain absolute.

23. Intrusion into signal-room, trespass in Telegraph Officer or obstruction

If any person:

a) Without permission of competent authority enters a building, or a portion thereof, housing equipment belonging to the Telegraph Authority or to a person licensed under this Act; or

b) Enters a fenced enclosure round such a telegraph office in contravention of any rule or notice not to do so, or

c) Refuses to quit such room to enclosure on being requested to do so by any officer or servant employed therein, or

d) Willfully obstructs or impedes any such officer or servant in the performance of his duty, he shall be punished with fine which may extend to five hundred rupees.

24. Unlawfully attempting to learn contents of messages

If any person does any of the acts mentioned in Section 23 with the intention of unlawfully learning the contents of any message, or of committing any offence punishable under this Act, he may (in addition to the fine with which he is punishable under Section 23) be punished with imprisonment for a term which may extend to one year.

Comments

Articles 23 and ***24*** of the Act, when taken together, deal with the protection of privacy rights. While ***Article 23*** outlines the cases where a person may be subjected to a penalty of Rs500 for intrusion into a telegraph office, refusing to leave that room even after being requested to do so, or obstructing the work of a telegraph official, ***Article 24*** extends the prior penalty, by adding imprisonment that may extend to an year, if the reason for that entry is to unlawfully attempt to learn the contents of messages.

25-D. Penalty for causing annoyance, etc.

Any person, including a Telegraph Officer, who uses any telephone, public or private, for causing annoyance or intimidation to any person, whether a subscriber or not, or for obnoxious calls shall, without prejudice to any other action which the Telegraph Authority is competent to make under this Act, be punishable with imprisonment for a term which may extend to three years, or with fine, or with both.

Comments

Article 25-D marks the punishment — imprisonment (up to three years), or a fine, or both — for "causing annoyance or intimidation" to any person over any telephone. Every person, including telegraph officers, falls under the gambit of this law; it is heartening to notice that no discrimination is exercised between government officials and the general public for protecting privacy rights.

SECTION H: CONCLUSION

Our journey through the massive inventory of Pakistani laws and their implications on privacy rights brings us to the conclusion that an immediate, concentrated and synergic effort needs to be taken by government departments concerned, the civil society, the media, the corporate sector and the general public to develop a rights-sensitive legal paradigm that supports societal development.

Although Pakistan has ratified major international treaties that recognize privacy as a fundamental human right and the Constitution of Pakistan reaffirms the inviolability of the same, the legal framework available to enact these laws in the true spirit is far from being satisfactory. During the study, it was surprising to find that Colonial acts, such as the Telegraphs Act of 1885, devised two centuries ago, are still active. Furthermore, it was appalling to notice the excessive powers bestowed upon the federal government for intrusion into the private lives of individuals for reasons of safeguarding national interests, national security or even the apprehension of crime.

It is high time for us to recognize that societal aspirations are hugely dependent upon the legal framework under which they are bound and that excessive limitations and irrational interference with the privacy of individuals act as a major deterrent in the development of individuality. Recognizing the importance bestowed upon privacy rights at different tiers in the international domain and the models of best practices adhered to, Pakistan must pick pace in developing justified and pragmatic procedures that shun actions that impede privacy rights in order to remain as a productive player in this globalized world.

It is recommended that a privacy protection act be passed in the parliament; that said act be created through a thorough consultative process amongst all major stakeholders. This act must incorporate privacy protection guidelines at par with international standards and must override all other laws that interfere with the essence of this act.

More specifically, we recommend that:

1. A privacy commission need to be constituted to guide privacy protection initiatives for citizens at the government level;

2. A comprehensive privacy protection index be developed to gauge temporal progress;

3. The judiciary should be given supreme authority in deciding cases where privacy is to be violated;

4. A 24/7 judicial tribunal be created to deal with privacy intrusion and surveillance imposed by the government;

5. A mass-awareness campaign be initiated to guide internet users regarding their privacy rights, cyber crimes and preventive measures;

6. A data protection act should be enacted and implemented;

7. Cyber Crimes legislation should be revised and enacted.

8. Judicial oversight should be extended to both before and after scenarios of surveillance. In other words data should be submitted and determined by a specialized court fully equipped to make determinations of this kind independently and impartially.

9. The scope of the allowable without notification surveillance must be limited to either those known terrorists or activists of terrorists organizations who have

a) Threatened to wage war against the state; and

b) Engaged in or planned on engaging in terrorist attacks against civilians
or

c) Those who are entrusted by the state to work in sensitive positions like nuclear or military installations, provided that they are made to sign a release and a waiver authorizing such surveillance and monitoring of their life.

10. In so far as the rest of the citizens are concerned, there should be mandatory user notification.

11. Specific exceptions ought to be made in the law for academics, non-violent dissidents and other outspoken members of society whose views may or may not conform to the officially acceptable state narrative. To monitor their correspondence on mere suspicion would be unfair and patently unconstitutional. The state should not be allowed to monitor law abiding citizens no matter what their thoughts or beliefs may be.

12. Instead of intruding into the private space of an individual, the state should attempt to enlist individuals who come in contact with the said individual. An email sent from suspected individual x to individual y should become admissible if individual y consents to release of the emails.

13. No effective safeguards exist to protect privileged relationships like doctor- patient confidentiality in a complete manner. This is an unacceptable fetter on freedom and privacy of an individual. Surveillance of emails, telephone calls and communications of a personal nature, whatever the nature of that personal interaction may be, should be exempt and penalties should exist for any such gross infringement on personal privacy.

14. Question of admissibility: No illegally obtained information should be admissible. Only data that is obtained legally conforming strictly to the requirements of the guidelines laid down by the court may be admitted into evidence.

15. Redress of grievances: If a person feels that he was unfairly monitored or feels aggrieved of an action of an investigating officer or surveillance and monitoring operative, should have occasion to approach the High Court and seek injunctive relief against the same. To this end, surveillance must be limited to a three (3) month period (unless the person shows cause) and every person who is monitored should be informed within six (6) months through the court.

Bytes for All (B4A), Pakistan is a human rights based think tank with a focus on Information and Communication Technologies (ICTs). It experiments and organizes debate on the relevance of ICTs for sustainable development and strengthening human rights movements in the country. At the forefront of the digital and Internet rights movement and struggle for democracy, B4A focuses on capacity building of human rights defenders on their digital security, online safety, and privacy.

Working on various important campaigns particularly against Internet censorship and surveillance in Pakistan, B4A focuses on cyberspace issues, awareness raising, and policy advocacy from civil liberties & human rights perspectives. The globally recognized and award winning Take Back The Tech! campaign is the flagship of B4A, which focuses on the strategic use of ICTs by women and girls to fight violence against women in Pakistan.

B4A partners and collaborates with a wide network of local & international human rights defenders and civil society organizations, and its team's commitment lies in protecting civil liberties in Pakistan.

Bytes for All, Pakistan
House 273, Street 17, F-10/2, Islamabad, Pakistan
+92 (51) 2110494-5 | www.bytesforall.pk
info@bytesforall.pk | @bytesforall

Design by Rabeea Arif
Layout by Sara Nisar