The Prevention of Electronic Crimes Act 2016: An Analysis

Eesha Arshad Khan*

Introduction

The advent of the digital age has created the need for a robust cybercrime legislation to be formulated by nation-states. However, many countries around the world are struggling with drafting comprehensive laws in this regard. Technological developments are outpacing the solutions proposed by state institutions, which aim to address the new challenges arising from the increasing use of digital media. Governments are also struggling to amend existing laws that seek to ensure the regulation of 'cybersecurity'.[1] In Pakistan, prior to the promulgation of the Prevention of Electronic Crimes Act (PECA) in 2016, the Electronic Transactions Ordinance 2002 (ETO) criminalised unlawful and unauthorised access to information. In the absence of a direct data protection legislation, the ETO provisions theoretically regulated data privacy and protection. It, however, does not regulate data protection directly but criminalises unlawful or unauthorised access to information.[2] It also envisages the establishment of a governmental authority to certify electronic documents and makes regulations for the privacy and protection of its users.[3]

The issues that have currently emerged due to the increasing usage of digital media call for the creation and implementation of a suitable legal framework that strives to protect the 'digital rights' of individuals.[4] It must not be forgotten that such laws are ultimately enacted for the protection of citizens. Any draconian provision that curtails the constitutional rights of citizens and bolsters tyrannical governmental power would defeat the spirit and letter of the law.

Despite near universal condemnation from alarmed human rights activists and politicians,[5] the PECA came into effect in August 2016. The enactment of this controversial statute ended a lengthy and fraught battle between the government and the various stakeholders who denounced it as "an incoherent mix of anti-speech, anti-privacy and anti-Internet provisions".[6] In a country like Pakistan, where there is relatively low digital literacy, an effective

* BA-LL.B (Hons) Lahore University of Management Sciences (LUMS).

[1] Measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack. 'Cybersecurity' (*Merriam*-Webster, 2018) <https://www.merriam-webster.com/dictionary/cybersecurity> accessed 31 October 2018.

[2] Electronic Transactions Act 2002, s. 36.

[3] Ibid, s. 43 (2) (e).

[4] Digital rights are basically human rights in the internet era. Rosamund Hutt, 'What Are Your Digital Rights?' (*World Economic Forum*, 2015) <https://www.weforum.org/agenda/2015/11/what-are-your-digital-rights-explainer> accessed 5 September 2018.

[5] ''Flawed' Cybercrime Bill Approved' (*DAWN*, 17 April 2015) <https://www.dawn.com/news/1176440> accessed 19 August 2018.

[6] Danny O'Brien, 'The Global Ambitions of Pakistan's New Cyber-Crime Act' (*Electronic Frontier Foundation*, 2016) <https://www.eff.org/deeplinks/2016/08/global-ambitions-pakistans-new-cyber-crime-act> accessed 18 September 2018.

law dealing with cybercrimes should have been drafted earlier and enforced, with the requisite acumen and insight to ensure that it remains within the constitutional framework.[7]

This review aims to analyse the PECA by placing it within Pakistan's constitutional framework and evaluating certain provisions, which are most likely to be in violation of fundamental rights granted in the Constitution of the Islamic Republic of Pakistan (Constitution). While there are several provisions in the PECA that are problematic, this review only focuses on a selected few. Firstly, the PECA is analysed in light of the due process provisions in the Constitution. Secondly, the restrictions, which the PECA imposes on free speech are analysed. Lastly, the review expounds the concept of the right to privacy in Pakistan and the potential harm that the PECA poses in this regard.

Background to the Law

The government campaigned for the law as a flagship element of its anti-terrorism agenda.[8] PECA was drafted as being part of the National Action Plan (NAP), which was developed in response to the APS attack of December 2014.[9] In lieu of the severity of the attack, the NAP was considered as a necessary step to eradicate terrorism. Government officials stressed that they needed an "unfettered ability to monitor, locate and prosecute alleged militant activity."[10] It is this particular desire that also permeated into all the other laws drafted in the aftermath of the APS attack. For example, in a defining moment in its war against terrorism, the Pakistani government responded to the attack by lifting the unofficial moratorium on the death penalty, asserting that only those convicted of terrorism would be executed.[11]

The situation of the post-APS Pakistan is comparable to that of a post-9/11 USA, wherein the US Congress passed the Patriot Act 2001,[12] within one month of the collapse of the World Trade Center. Similarly, in the UK, two months after 9/11, the Anti-Terrorism, Crime and Security Act was passed in 2001.[13] Both these laws were criticized for threatening the civil liberties of resident nationals.[14] In view of the aforementioned examples, it can be stated that the fundamental rights of the citizens were curtailed simply by spreading a panic. As per the Humanitarian Policy Group, the Pakistani state tends to prioritise national security at the expense of the constitutional safeguards and humanitarian considerations, especially in situations of crisis

---

[7] 'Pakistan ranked low in digital literacy' (*The Frontier Post*, 18 July 2018) <https://thefrontierpost.com/pakistan-ranked-low-in-digital-literacy> accessed 19 August 2018.

[8] 'The Prevention of Electronic Crimes Bill 2015 - An Analysis' (*Article 19*, 2016) <https://www.article19.org/data/files/medialibrary/38416/PECB-Analysis-June-2016.pdf> accessed 16 May 2018.

[9] Ibid.

[10] Furqan Mohammed, 'PECA 2015: A Critical Analysis of Pakistan's Proposed Cybercrime Bill' (2016) 15 (1) *Journal of Islamic and Near Eastern Law* 71.

[11] 'APS: One Year After' (*DAWN*, 16 December 2015) <https://www.dawn.com/news/1226622> accessed 5 September 2018.

[12] 'The Patriot Act - Constitutional Rights Foundation' (*Constitutional Rights Foundation*, 2018) <http://www.crf-usa.org/america-responds-to-terrorism/the-patriot-act.html> accessed 19 August 2018.

[13] 'Case Study: ANTI-TERRORIST LEGISLATION POST SEPT. 11' (*BBC World Service*) <http://www.bbc.co.uk/worldservice/people/features/ihavearightto/four_b/casestudy_art09.shtml> accessed 19 August 2018.

[14] Ibid.

when a response is needed on an emergency basis.[15] Therefore, in order to identify which fundamental rights are being infringed, it is imperative to analyse the cybercrime statute from a constitutional perspective in order to ensure that it does not negatively impact the rights of citizens.

The Vagueness and Over Breadth in the Laws

The due process of law is a constitutional guarantee that generally relates to fair treatment through the normal judicial system.[16] This specifically relates to a citizen's entitlement to notice of a charge and hearing before an impartial judge.[17] An understanding of due process of law is necessary in order to comprehend the significance of constitutional rights. This is because without this guarantee there might be rampant abuse of power by the government.

Under Article 4 of the Constitution, every citizen has the right to be treated according to the law.[18] This means any invasion upon the rights of a citizen – whether by a private or public individual or body – must be justified with reference to some law of the country. Another relevant provision is Article 10-A which entitles citizens to a fair trial and due process. This provision is limited to criminal charges only.[19]

These constitutional guarantees have been subject to interpretation by the judiciary. The scope of the doctrine of due process was first discussed in the *Begum Shorish Kashmiri* case.[20] Along with discussing the meaning of the word 'law', the court also affirmed that it was the constitutional right of every citizen to be tried in accordance with it.[21] Herein, this word was not confined to a statute and was used in a generic sense as something that should be in accordance with the judicial principles laid down from time to time by superior courts.[22] Thus, the Supreme Court ruled that Article 2 of the 1962 Constitution should be interpreted "according to the accepted forms of legal process"[23] and so "in this sense, it is as comprehensive as the American due process clause."[24] Verily, it was in this case that the scope and ambit of due process was expanded from merely procedural due process to substantive due process.[25] Therefore, it can be concluded that due process protections in Pakistan guarantee an adherence to the ethical spirit of

[15] 'HPG Policy Brief 36' (*Humanitarian Policy Group*, 2009) 1 <https://web.archive.org/web/20120606093049/http://www.odi.org.uk/resources/docs/4854.pdf> accessed 5 September 2018.
[16] 'Due Process of Law - Magna Carta: Muse and Mentor' (*Library of Congress*, 2018) <http://www.loc.gov/exhibits/magna-carta-muse-and-mentor/due-process-of-law.html> accessed 19 August 2018.
[17] Dhruvkumar S. Chauhan, 'Evolution of "Due Process of Law" under Indian Constitution: A Special Comparative Analysis with the Concept under Pakistani Constitution' (2016) (11) (2) *Imperial Journal of Interdisciplinary Research* 2 <https://www.onlinejournal.in/IJIRV2I11/295.pdf> accessed 31 October 2018.
[18] The Constitution of Islamic Republic of Pakistan 1973, art. 4.
[19] Ibid, art. 10-A.
[20] *Government of West Pakistan and another v Begum Agha Abdul Karim Shorish Kashmiri* PLD 1969 SC 14.
[21] Ibid, 16.
[22] Ibid.
[23] (n 20) 14. Article 2 of the Constitution of 1962 is now known as Article 4 in the Constitution of 1973.
[24] Ibid.
[25] (n 21).

the law, which means that among other things, a law must uphold the liberties and rights of the citizenry.[26]

With regards to PECA, it can be stated that it offends the inalienable guarantees of the due process provisions provided in the Constitution. Both are elements that can cause the legislation to be struck down. The drafting of the law is such that it is difficult to decipher exactly what amounts to a criminal conduct. For example, under the definitions section, certain terms have been defined in a very subjective manner.[27] The word 'act' has been defined under the statute as 'a series of acts' without elaborating as to what constitutes an 'act' under the said provision.[28] Similarly, dishonest intention has been defined as having an "intention to cause injury, wrongful gain or wrongful loss or harm to any person or to create hatred".[29] This definition has been made extremely subjective due to the inclusion of the words "to create hatred".[30] Section 10 entails the description of cyber-terrorism, which is a crucial concept for the purposes of this Act. However, it has been criticized that this concept has been defined too broadly.[31] Critics are of the view that cyber-terrorism offences must be clearly linked to "violence and the risk of harm and injury".[32] However, section 10 (b) declares the advancement of "inter-faith, sectarian or ethnic hate" as a qualifier for cyber-terrorism.[33] Hence, the language of the provision tends to confuse terrorism with offences relating to the incitement of violence or hostility.

Generally, ambiguous and technical provisions in the law are usually tested on the basis of the vagueness doctrine.[34] This doctrine requires criminal laws to explicitly state what exactly amounts to a punishable conduct and any law, which is in violation of this doctrine is said to be void on the grounds of vagueness.[35] Several provisions of this Act can be rendered void as they are likely to offend the due process provisions guaranteed in the Constitution. An example of this is section 48, which is a general provision relating to the prevention of electronic crimes.[36] This provision gives the government and Pakistan Telecommunications Authority (PTA) the power to issue directives to service providers in the interest of preventing an offence under the Act.[37] Once again, the provision lacks precision and any restrictions whatsoever.[38] The lack of any safeguards gives PTA unbridled discretion to issue additional rules that would just exacerbate various problems, especially those relating to the curtailment of free speech.

---

[26] Abhinav Chandrachud, *The Due Process of Law* (2nd edn, Eastern Book Company 2011) 1-2.
[27] (n 8), 10.
[28] Prevention of Electronic Crimes Act 2016, s. 2 (1) (i) (a).
[29] Ibid, s. 2 (1) (xvi).
[30] Asad Baig, 'Prevention of Electronic Crimes Bill 2016 – Implications for Investigative and Public Interest Journalism' (*Media Matters for Pakistan*, 2016) <http://mediamatterspakistan.org/prevention-of-electronic-crimes-bill-2016-implications-for-investigative-and-public-interest-journalism> accessed 16 May 2018.
[31] (n 28) s. 10.
[32] (n 8), 14.
[33] (n 28) s. 10 (b).
[34] Faisal Daudpota, 'An Examination of Pakistan's Cybercrime Law' (2016) *SSRN* 14 <http://dx.doi.org/10.2139/ssrn.2860954> accessed 16 May 2018.
[35] Ibid.
[36] (n 28) s. 48.
[37] PTA, a government institution, established in 1996 to regulate the establishment, operation and maintenance of telecommunication systems, and the provision of telecom services.
[38] (n 36).

Section 31 of the Act discusses "expedited preservation and acquisition of data".[39] It allows an authorised agent to require a person to hand over data without producing a court warrant if it is believed that it is "reasonably required" for a criminal investigation.[40] This can be termed as a blanket authorisation provision that gives the executive direct authority to take action without any judicial oversight or scrutiny.[41] In addition to this, no test as to what amounts to a reasonable requirement is provided in the section. This is problematic because the lack of requisite checks and balances affords the executive a discretionary power that can be used to violate fundamental rights. This can consequently rob a citizen of his right to be treated in accordance with the due process of law.[42] Such a provision can, therefore, be subject to misuse and exploitation in order to achieve certain political agendas and suppress any form of lawful debate or dissent.

Freedom of Speech

PECA has faced a lot of criticism for violating the fundamental right of freedom of speech under Article 19 of the Constitution.[43] Freedom of speech and press are fundamental rights that signify the cornerstones of democratic institutions. However, such freedom is subject to any reasonable restrictions that may be imposed by law.[44] While, there can be no absolute test for reasonableness of restrictions imposed by law, as a general rule of thumb, it is for the courts to decide whether, under the given circumstances, a restriction is reasonable or not.[45]

Firstly, one of the most pressing concerns relates to whether some of the powers given to authorities under PECA should lie with them in the first place. For instance, section 37 of the Act discusses unlawful online content. It gives vast powers to PTA to block or remove online content, thereby restricting the right to freedom of expression.[46] Historically speaking, PTA is notorious for its casual yet frequent dalliances with censorship, and for its arbitrary blocking and removal of content.[47] This is problematic at two levels. Firstly, the specific cases related to the right to freedom of speech that fall within or outside the exceptions listed in Article 19 are left to the sole discretion of the executive authority of PTA. PTA has the absolute power to decide as to how Article 19 is to be interpreted and applied. PTA also has the authority to determine the content that may or may not be accessed by internet users in the country.[48] Authorised personnel

[39] (n 28) s. 37.
[40] Ibid.
[41] (n 34), 21.
[42] Ibid.
[43] (n 8) 12.
[44] 'Article 19 and threat to media' (*The News*, 3 May 2018) <https://www.thenews.com.pk/print/311886-article-19-and-threat-to-media> accessed 12 November 2018.
[45] *Tofazzal Hossain v Government of West Pakistan* PLD 1969 Dacca 589.
[46] (n 28), s. 37.
[47] In April 2015, PTA also blocked a political forum Siasat.PK for harboring an anti-government stance. Siasat.pk is a famous platform where people express their criticism against the government. The case was reported in Pakistani media and after receiving public pressure, the government restored the forum. Haroon Baloch, Maria Xynou and Arturo Filasto, 'Internet Censorship in Pakistan: Findings From 2014-2017' (*Open Observatory of Network Interference*, 2017) <https://ooni.torproject.org/post/pakistan-internet-censorship/#censorship> accessed 16 September 2018.
[48] 'Pakistan's Cybercrime Law: Boon or Bane?' (*Heinrich Böll Foundation*, 2018) <https://www.boell.de/en/2018/02/07/pakistans-cybercrime-law-boon-or-bane> accessed 16 May 2018.

from the PTA have the power to remove any content that they believe is immoral, anti-state, against any country considered to be an ally of Pakistan, or politically unacceptable.[49] This shows that both legislative and judicial functions have been placed in the domain of a single executive authority. One must also note that section 37 simply reiterates the restrictions relating to freedom of speech, which have been discussed in Article 19 of the Constitution.[50] Instead of adopting a more nuanced approach towards cybercrimes and providing laws that secure the interest of citizens and safeguard fundamental rights, the legislature has focused on providing a law that prioritises national security.

Moreover, section 37 allows complainants to file petitions with the PTA to block any content in question.[51] PTA can act unilaterally against such content, without acquiring a court order. This indirectly provides the State with a mechanism to deal with and block content that it deems as unpalatable. For example, the government might block access to some political content under the pretext of preventing harm.[52] According to a transparency report issued by Facebook, 177 pieces of content have already been restricted from viewership in the country based on requests forwarded by the PTA for violating "local laws prohibiting blasphemy and condemnation of the country's independence".[53]

There are several other provisions of the Act that threaten free speech. For example, section 9 discusses the glorification of an offence and specifies the types of offences and activities for which this is criminalised.[54] However, this section has been drafted in overly broad terms and breaches international standards of freedom of speech, if not Article 19 of the Constitution. It is a textbook example of a provision that has a 'chilling effect' on free speech. In a legal context, a chilling effect is the discouragement of the legitimate exercise of legal rights by the threat of legal sanction.[55] Normally, this terminology is discussed in the USA as being linked to the First Amendment. In the US Supreme Court case of *Reno v ACLU*, the constitutionality of two provisions of a statute was challenged.[56] The Supreme Court held that the statute violated its First Amendment because the regulations amounted to a content-based blanket restriction of free speech. Justice John Paul Stevens wrote that the vagueness of the statute was a matter of special

[49] 'Prevention of Electronic Crimes Act 2015: Curbs against Cyber Terrorism or 'Freedom of Speech'?' (*Daily Pakistan Global*, 17 April 2015) <https://en.dailypakistan.com.pk/technology/prevention-of-electronic-crimes-act-2015-against-cyber-terrorism-or-freedom-of-speech> accessed 16 May 2018.
[50] The Constitution of the Islamic Republic of Pakistan, art. 19.
[51] (n 28).
[52] 'The Baloch Hal' is an example of crushing political dissent of an ethnic group by the State. PTA blocked the website in 2010 and the ban continues. The Baloch Hal was the first online English language newspaper for the province of Balochistan. Because of its liberal point of view and touching upon the sensitive conflict related issues in Baluchistan, PTA put it offline. 'Censorship Returns to Pakistan' (*Huffington Post*, 2012) <https://www.huffingtonpost.com/malik-siraj-akbar/pakistan-censorship_b_1302660.html> accessed 9 November 2018.
[53] 'Facebook Says Blocking Dawn.Com Post in Pakistan Was 'Mistake'' (*DAWN*, 11 May 2018) <https://www.dawn.com/news/1407047/facebook-blocks-dawncom-post-in-pakistan-based-on-local-law> accessed 16 May 2018, 'Transparency' (*Facebook*, 2018) <https://transparency.facebook.com/government-data-requests/country/PK> accessed 19 August 2018.
[54] (n 28) s. 9.
[55] 'Reno v American Civil Liberties Union, 117 S.Ct. 2329, 138 L.Ed.2D 874 (1997)' (*Cornell University Law School*, 2018) <https://www.law.cornell.edu/supct/html/96-511.ZS.html> accessed 18 September 2018.
[56] Ibid.

concern because it related to a content-based regulation of speech.[57] The vagueness of such a regulation raised special First Amendment concerns because of its chilling effect on free speech. Herein, the 'chilling effect' would have been the discouragement of the exercise of an individual's right to free speech. Similarly, section 9 of the PECA would most likely stifle any sort of debate on issues of national security, terrorism or even of a mere public interest. Specifying that this section relates to "a crime related to terrorism" and "activities of proscribed organisations" does not resolve the threat it poses to the freedom of speech and press.[58]

In 2015, in a watershed moment for free speech online, the Indian Supreme Court struck down section 66-A of the Information Technology Act 2000 on the grounds of violation of freedom of speech, guaranteed under Article 19(1)(a) of the Constitution of India.[59] It was held that the section did not meet the criterion of 'reasonable restriction'. The phenomenon of 'chilling effect' was discussed by the court as the rationale for striking down the overbroad and vague statutory provision.[60] This action shows the importance of the right to freedom of speech. Furthermore, Pakistan, just like India, has signed and ratified the International Covenant on Civil and Political Rights (ICCPR).[61] The government is therefore bound to ensure adherence and implementation of its provisions, especially those relating to freedom of expression and speech.

The Right to Privacy

The Constitution of Pakistan enshrines the right to privacy as a fundamental right under Article 14(1).[62] Moreover, Article 17 of the ICCPR, to which Pakistan is a signatory, states that "no one shall be subject to arbitrary or unlawful interference with his privacy, family or correspondence."[63] The scope and interpretation of Article 14 was discussed by the Supreme Court in the case of *Mohtarma Benazir Bhutto v President Pakistan*.[64] Affirming the dignity of man and privacy home as inviolable, the Court went on to clarify that an individual's privacy is vulnerable even outside his home and the emphasis was on the right regardless of the location. The term 'home' was construed as being a space wherein an individual enjoys personal freedom and feels secure. The Court went on to hold that subject to law, the privacy of person could not be intruded in public spaces.[65]

---

[57] Ibid.
[58] (n 28), s. 9.
[59] Owais Farooqui and Aftab Alam, 'Shreya Singhal V. Union of India: Case Analysis' (2015) 1 (1) *International Journal of Law* 58.
[60] Ibid, 56.
[61] As per articles 18 and 19 of the ICCPR, the Pakistani government is bound to uphold the right to freedom of thought, conscience and religion and the right to hold opinions without interference. 'International Covenant on Civil and Political Rights' (*United Nations Human Rights*, 1966) <https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx> accessed 10 September 2018
[62] The Constitution of the Islamic Republic of Pakistan, art. 14(1). 'the dignity of man and, subject to law, the privacy of home, shall be inviolable'.
[63] (n 61).
[64] PLD 1998 SC 388.
[65] Ibid, 621.

A report published by Privacy International, reveals that there are no direct data protection authorities or laws in Pakistan.[66] In the absence of a direct data protection legislation, data privacy and protection was theoretically regulated through provisions of the Electronic Transactions Ordinance 2002 and The Freedom of Information Ordinance 2002.[67] PECA also contains a number of provisions related to data privacy. However, these are intended to grant government agencies access to the private data of citizens or to restrict citizens from gaining access to government data.[68] Several provisions of the statute make it a crime for anyone to gain unauthorised access to any information system or data or copying or transmission of critical infrastructure data.[69]

PECA also tends to encroach upon the right to privacy, as certain provisions therein are intended to grant the PTA and other law enforcement agencies access to the private data of citizens, along with restricting citizens from gaining access to government data. Provisions of the Act allow for the retention of data by Internet Service Providers (ISPs), for the supply of data to foreign entities, and the empowerment of officials to force citizens to give up their private information (which could be used against them in criminal investigations).

As per, section 31 of the Act, a law enforcement agency may require an individual to hand over data without producing any court warrant if it is believed that it is "reasonably required" for a criminal investigation.[70] The provision empowers an officer to take this action as per his discretion and requires for him to only bring this to the notice of a court within 24 hours after the acquisition of the data.[71] Thus, in cases involving "cyberterrorism", which is vaguely defined, the officer can search, seize, and retain data without a warrant and notify the court within 24 hours of its seizure. The right to privacy *vis a vis* the power to enter, search, and seize was discussed in *Mehram Ali v Federation of Pakistan*, wherein the Supreme Court declared section 10 of the Anti-Terrorism Act (ATA) to be unconstitutional.[72] Section 10 of the ATA, empowered an authorised official, on him being satisfied that there were reasonable grounds for suspecting that a person had in his possession some written material or recording in contravention of section 8 of the ATA, to enter and search the premises, and seize any suspicious material or recording.[73] The Supreme Court held that while there was no doubt that right to privacy was subject to reasonable restriction but such law was supposed to be reasonable and in conformity with the constitutional mandate.[74]

Section 32 of the Act requires ISPs to retain specified traffic data for a minimum of one year and subject to the demands of the PTA, provide that data to an investigation agency or authorised agent.[75] Such an indiscriminate requirement for service providers to retain data

[66] 'State of Privacy Pakistan' (*Privacy International*, 2018) <https://privacyinternational.org/state-privacy/1008/state-privacy-pakistan> accessed 10 September 2018.
[67] Ibid.
[68] Ibid.
[69] (n 28) s. 3-8.
[70] Ibid, s. 31.
[71] Ibid.
[72] PLD 1998 SC 1445.
[73] Ibid, 1462.
[74] Ibid, 1488.
[75] (n 28) s. 32.

breaches the international standards of the right to privacy. The requirement of storing it for one year is significantly longer than the previous requirement of 90 days, as envisaged in an earlier draft of the Act. This requirement is deemed quite problematic as it fosters the growth of conditions under which a highly invasive blanket surveillance of populations would be able to take place.[76] In 2014, a UK High Court declared the Data Retention and Investigatory Powers Act 2014 (DRIPA) to be unlawful.[77] DRIPA was challenged on the grounds of violation of the right to privacy. Furthermore, it was found to be inconsistent with Article 8 of the European Convention on Human Rights, which relates to the right to respect for one's private and family and the protection of personal data.[78] In the same year, the Court of Justice of the European Union noted that the retention of data may allow "very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained".[79] Thus, it was concluded that such retention was a disproportionate interference with the right to privacy.[80] The same arguments can be made to challenge the constitutionality of this particular section in Pakistan. The practical implications of this particular provision are already beginning to materialise. From January 2017 to June 2017, the Pakistani government sent 1,050 requests for data to Facebook, compared to 2016 when only 719 requests were made.[81] However, nobody knows the reasons as to why such access was requested and whether this law was actually used to prevent tangible harm from materialising.

Section 42 of the Act discusses international cooperation in the context of data sharing. Herein, sweeping powers are delegated to the government when it comes to sharing information with foreign entities.[82] This is troubling as the language of the provision allows for unilateral cooperation between the government and other countries and their agencies. Furthermore, sub-section 2 permits the government to share data obtained under this Act with foreign or international agencies.[83] This is extremely alarming because this entire process entails no recourse to judicial authorisation or oversight. Under this provision, once sensitive private data has been left at the disposal of the government, it could be used by foreign entities as they deem fit.[84] Moreover, the language of the section is a product of poor drafting. A plain reading of the law might lead one to conclude the law of information sharing in Pakistan primitive and undeveloped, as the provision does not even discuss any accountability mechanisms or any process of administrative and judicial oversight.

Conclusion

[76] 'How Not to Draft Legislation: Prevention of Electronic Crimes Bill from Bill to Act' (*Medium*, 2016) <https://medium.com/privacy-international/prevention-of-electronic-crimes-from-bill-to-act-what-has-been-achieved-63660230c124> accessed 16 May 2018; (n 27).
[77] 'DRIPA Struck Down by High Court in Judicial Review Challenge' (*Focus on Regulation*, 2015) <https://www.hlregulation.com/2015/07/24/dripa-struck-down-by-high-court-in-judicial-review-challenge> accessed 16 May 2018.
[78] Ibid.
[79] 'All General Obligations to Retain Traffic Data Found Illegal under EU Law' (*Intellectual Property Watch*, 21 December 2016) <http://www.ip-watch.org/2016/12/21/general-obligations-retain-traffic-data-found-illegal-eu-law> accessed 16 May 2018.
[80] Ibid.
[81] (n 53).
[82] (n 28) s. 42.
[83] Ibid, s. 42 (2).
[84] (n 61).

Drafted within the national security framework, PECA compromises multiple constitutional rights under the guise of curbing cybercrime, the likes of which include common digital threats such as fraud, online stalking, and harassment.[85] When it was finally pushed through the Parliament, the public was introduced to a poorly drafted law laced with ambiguity, vagueness, and over breadth.[86] The Act criminalises free speech and delegates massive sweeping powers to the Pakistani law enforcement authorities.[87] In pure constitutional terms, PECA violates Articles 4, 10-A, 14, and 19 of the Constitution of the Islamic Republic of Pakistan 1973.[88] The aforementioned articles relate to certain universal fundamental rights, which are the cornerstones of a democratic polity. Therefore, it is important that they should not be side lined in the name of national security.

Owing to the recent wave of cybercrime laws globally, most nations have struggled to frame them within their existing legal structures. As of now, there is a dire need to revamp the PECA in order to ensure that the citizen's rights to privacy and freedom of speech are not compromised. PECA needs to be rebuilt from the ground up so as to preserve the due process rights of those who are tried under it. Moreover, the law must be drafted in compliance with the ICCPR. Cybercrime laws are a new development and the existing laws need to be able to address a wide spectrum of problems relating to online spaces. With cyber-attacks and data leaks like the Cambridge Analytica Scandal, Careem, and PITB-NADRA data breaches becoming a norm, undoubtedly, there is no disagreement that comprehensive cybercrime laws are the need of the hour.[89] However, it is important that they are enacted in such a manner that upholds the rights and freedoms of the citizenry, instead of violating them.

---

[85] Ibid.

[86] 'Vagueness in Cybercrime Law' (*The Express Tribune*, 29 August 2016) <https://tribune.com.pk/story/1172081/vagueness-cybercrime-law> accessed 3 September 2018.

[87] Ibid.

[88] Article 4 of the Constitution of 1973 relates to the universal law of due process; Article 10-A relates with the right to fair trial; Article 14 deals with the dignity of a person and the privacy of home, and Article 19 deals with the freedom of speech.

[89] The Facebook–Cambridge Analytica data scandal relates to the collection of personally identifiable information of 87 million Facebook users that Cambridge Analytica began collecting in 2014. It is alleged that the date was used to attempt to influence voter opinion on behalf of politicians who hired them. The way that Cambridge Analytica collected the data has been deemed inappropriate and Facebook has issued a public apology since then. In the same vein, in February 2018, hackers accessed the names, email addresses, phone numbers and trip data of anyone who signed up for Careem, a transportation network company based in Dubai, with operations in over 100 cities in 14 countries. Sam Meredith, 'Here's everything you need to know about the Cambridge Analytica scandal' (*CNBC*, 21 March 2018) <https://www.cnbc.com/2018/03/21/facebook-cambridge-analytica-scandal-everything-you-need-to-know.html> accessed 3 September 2018; 'Dubai's Careem Admits to Data Breach Of 14 Million Users' (*Khaleej Times*, 24 April 2018) <https://www.khaleejtimes.com/nation/dubai//dubais-careem-admits-to-data-breach-of-14-million-users> accessed 18 September 2018.