DigitalRightsFoundation

"KNOW YOUR RIGHTS"

Removal and Blocking of Unlawful Online Content (Procedure, Oversight and Safeguards) Rules, 2020: Legal Analysis

Digital Rights Foundation

November 30, 2020

www.digitalrightsfoundation.pk

Introduction

The 'Removal and Blocking of Unlawful Online Content (Procedure, Oversight and Safeguards), Rules, 2020 (hereinafter as the "**Rules"**) have been notified under section 37 (2) of the Prevention of Electronic Crimes Act, 2016 (hereinafter as the **"PECA"**) and published in the Official Gazette on 20 October, 2020.[1] Under these Rules, the Pakistan Telecommunication Authority (hereinafter as the **"PTA"**) is the designated Authority, vested with powers to remove and block content on the internet. This legal analysis will highlight the jurisdictional and substantive issues with the Rules in light of Constitutional principles and precedent as well as larger policy questions.

Digital Rights Foundation (hereinafter as **"DRF"**) has registered its opposition to the Rules in light of the larger implications it will have on freedom of expression, right to privacy and the digital economy.[2] We maintain that the powers assumed by the PTA under the Rules are ultra-vires of the Parent Act, PECA, and constitutional powers to block speech content on the internet. We maintain that section 37 of PECA, which gives powers to the PTA to remove or block Online Content, in its form and application, is violative of the freedom of expression and right to information enshrined in the Constitution of Islamic Republic of Pakistan, 1973 (hereinafter as the "**Constitution**") and also contravenes Pakistan's international law commitments. DRF's advocacy and positions are focused on the eventual repealing of the said section through either legislative amendment or judicial review, striking it down on constitutional grounds.

---

[1] The Rules can be accessed on the official website of the Ministry of Information Technology: https://moitt.gov.pk/SiteImage/Misc/files/Social%20Media%20Rules.pdf.

[2] "Digital Rights Foundation is gravely concerned by the the Removal and Blocking of Unlawful Online Content (Procedure, Oversight and Safeguards), Rules 2020," *Digital Rights Foundation*, November 19, 2020, https://digitalrightsfoundation.pk/digital-rights-foundation-is-gravely-concerned-by-the-the-removal-and-blocking-of-unlawful-online-content-procedure-oversight-and-safeguards-rules-2020/.

Context and Background

Earlier this year, the Federal Government notified the Citizens Protection (Against Online Harm) Rules, 2020 (hereinafter as the **"Harm Rules"**) which were unanimously condemned and rejected by digital rights groups and civil society.[3] The sudden appearance of the Harm Rules and the secretive and exclusionary process of drafting them were questioned by civil society.[4] The Harm Rules themselves were criticized for restricting free speech and threatening the privacy of Pakistani citizens. Partly as a result of the sharp criticism, the implementation of the Harm Rules was suspended and the Prime Minister of Pakistan promised to initiate a broad-based consultation on regulating Online Content. DRF, along with other civil society organisations, boycotted the consultation process conducted by the Ministry of Information Technology & Telecommunication (MoITT) on grounds that the Harm Rules were not formally de-notified by the Government.[5]

Despite challenges in High Courts across the country,[6] the consultation process initiated in June 2020 was based on the earlier draft of the Harm Rules and the fundamentally flawed section 37 of PECA.[7] We reiterated our concerns and reservations with the entire process even at that time highlighting how the consultative process is devoid of any meaningful public engagement. Our worst fears have been confirmed since then as the Government has failed to share the draft of the newly formulated Rules with any of the stakeholders, including social

---

[3] "DRF Condemns Citizen's Protection (Against Online Harm) Rules 2020 as an Affront on Online Freedoms," *Digital Rights Foundation*, February 13, 2020, https://digitalrightsfoundation.pk/drf-condemns-citizens-protection-against-online-harm-rules-2020-as-an-affront-on-online-freedoms/.

[4] "No Consultation without withdrawal of cabinet approval of Online Protection (Against Online Harm) Rules 2020," *Digital Rights Foundation*, March 1, 2020, https://digitalrightsfoundation.pk/no-consultation-without-withdrawal-of-cabinet-approval-of-online-protection-against-online-harm-rules-2020/.

[5] "Comments on the Consultation & Objections to the Rules," *Digital Rights Foundation*, July 1, 2020, https://digitalrightsfoundation.pk/comments-on-the-consultation-objections-to-the-rules/.

[6] "IHC issues notice to IT ministry to justify Citizen Protection Rules," *The Nation*, February 24, 2020, https://nation.com.pk/24-Feb-2020/ihc-notices-it-ministry-to-justify-new-social-media-regulations. Hasnaat Malik, "IHC moved against new rules for regulating social media," *The Express Tribune*, August 15, 2020, https://tribune.com.pk/story/2259646/ihc-moved-against-new-rules-for-regulating-social-media.

[7] Ramsha Jahangir, "Govt begins consultation on online harm rules," *Dawn*, June 3, 2020, https://www.dawn.com/news/1560952.

media companies who participated in the process. These new Rules were also only available once published on the MoITT's website on 18 November, 2020, and saw the Government repeating the same mistakes in the new version. The Government has failed to address the concerns raised by civil society and the entire 'consultation' process has merely been an eyewash to legitimise the Rules. Under a new name, the Government has presented a fundamentally similar version of the previously rejected and condemned Harm Rules.

Summary of the Rules and Analysis

The Rules have been formulated to provide for safeguards, process and mechanism for exercise of powers by PTA with respect to removal of or blocking access to "unlawful online content". The Rules are to come into force at once.

Rule 4 - Freedom of speech and expression:

Rule 4 prescribes that every person or organization has the freedom to express themselves by disseminating any Online Content on any Information System. However, this is not an absolute right and restrictions can be placed if they are necessary in the interest of:

1. **Glory of Islam:** The expression includes all offences that fall under chapter XV of the Pakistan Penal Code, 1860 (hereinafter as the **"PPC"**).[8]
2. **Integrity, security and defence of Pakistan**: This expression has been given the same meaning as under Article 260 of the Constitution[9]. In addition, the expression also includes "disseminating information that harms the reputation of the Federal or Provincial Government or any person holding public office" as well as "transmission of information which brings hatred, contempt or disaffection towards the Federal or Provincial Government."

[8] These include sections 295 (Injuring or defiling place of worship, with Intent to insult the religion of any class), 295-A (Deliberate and malicious acts intended to outrage religious feelings of any class by insulting Its religion or religious beliefs), 295-B (Defiling, etc., of Holy Qur'an), 295-C (Use of derogatory remarks, etc., in respect of the Holy Prophet), 296 (Disturbing religious assembly), 297 (Trespassing on burial places, etc.), 298 (Uttering words, etc., with deliberate intent to wound religious feelings), 298-A (Use of derogatory remarks, etc., in respect of holy personages), 298-B (Misuse of epithets, descriptions and titles, etc., reserved for certain holy personages or places), and 298-C (Person of Quadiani group, etc., calling himself a Muslim or preaching or propagating his faith)

[9] The term "security of Pakistan" has been defined in article 260 of the Constitution to include "*the safety, welfare, stability and integrity of Pakistan and of each part of Pakistan, but shall not include public safety as such*."

3. **Public order:** This term includes all offences under chapter XIV of PPC[10] and dissemination of fake or false information that threatens public order, public health and public safety.

4. **Decency and morality:** Contains offences under sections 292, 293, 294 and 509 of PPC.[11]

Rule 4 (2) states that the Rules will prevail and take precedence over "any contrary Community Guidelines" issued by a service provider.

- **Analysis:**

At the outset, we submit that the rule-making power and for that matter, the power to make any kind of subordinate legislation, does not ordinarily include the power to change the ordinary meaning of the words used in the enabling statute. As was held in the case of Mehmood Tahsin v. Ejaz Hussain[12] *"where an expression has been used but not defined in the enabling Act, that expression is presumed to have been used in its ordinary sense and the rules cannot give it an artificial meaning."* However, the Rules define certain terms and phrases that were used in section 37 of PECA but left undefined, such as "Glory of Islam," "Integrity, Security and defence of Pakistan," "Public Order" and "Decency and Morality." We submit that the rule-making Authority (PTA) has no powers to define terms that were used in the

[10] Chapter XIV, "Offences Affecting the Public Health, Safety, Convenience, Decency and Morals", includes the following sections: 268 (Public nuisance), 269 (Negligent act likely to spread infection of disease dangerous to life), 270 (Malignant act likely to spread infection of disease dangerous to life), 271 (Disobedience to quarantine rule), 272 (Adulteration of food or drink intended for sale), 273 (Sale of noxious food or drink), 274 (Adulteration of drugs) , 275 (Sale of adulterated drugs), 276 (Sale of drug as a different drug or preparation), 277 (Fouling water of public spring or reservoir), 278 (Making atmosphere noxious to health), 279 (Rash driving or riding on a public way), 280 (Rash navigation of vessel), 281 (Exhibition of false light, mark or buoy), 282 (Conveying person by water for hire in unsafe or overloaded vessel), 283 (Danger or obstruction in public way or line of navigation), 284 (Negligent conduct with respect to poisonous substance), 285 (Negligent conduct with respect to fire or combustible matter), 286 (Negligent conduct with respect to explosive substance), 287 (Negligent conduct with respect to machinery), 288 (Negligent conduct with respect to pulling down or repairing buildings), 289 (Negligent conduct with respect to animal), 290 (Punishment for public nuisance in cases not otherwise provided for), 291 (Continuance of nuisance after injunction to discontinue), 292 (Sale, etc., of obscene books, etc.:), 293 (Sale, etc., of obscene objects to young person), 294 (Obscene acts and songs), 294-A (Keeping lottery office), 294-B (Offering of prize in connection with trade, etc.),

[11] Section 509: "Insulting modesty or causing sexual harassment".

[12] PLD 1965 SC 618.

enabling/parent Act i.e. PECA. Even otherwise, a sub-statutory legislation cannot define or interpret Constitutional expressions.

Moreover, the term "integrity, security and defence of Pakistan'' has been given a meaning much wider than even under Article 260 of the Constitution and has been expanded to provide reputational protection to the Federal and Provincial governments. We would like to remind the government that the power to enlarge, expand and change meanings of these Constitutional expressions has not been delegated or given to the rule-making Authority and therefore, this entire exercise is in contravention of the enabling Act as well as the Constitution.

It should also be noted that sub-statutory rules cannot impose or create new restrictions beyond the scope of the parent Act. Protecting the reputation of the Federal or Provincial Government is not a ground recognized under PECA, or even the Constitution, on which freedom of expression can be restricted. It should also be noted that even the defamation law under PECA (section 20) offers reputational protection to 'natural persons' alone and does not extend to legal persons or, for that matter, the Federal or Provincial Government. Therefore, the criteria laid down under Rule 4 exceeds the existing ambit and is ultra vires of the parent Act and the powers granted under section 37 (2) of PECA.[13]

We also face difficulty in understanding how the government draws a nexus between "integrity, security and defence of Pakistan" and harming the reputation of the Federal and Provincial Government. In his book titled "Judicial Review of Public Actions, Second Edition," Justice (retd.) Fazal Karim defines the expression 'security or defence of Pakistan' as *"defence of the realm, protection of the State's secrets and instruments of the State's defence."*[14] Even under Indian case law, "security" has been defined to include "*those aggravated forms of prejudicial activities which endanger the very existence of the State but do not include ordinary breaches of the peace.*[15]" However, the Rules equate the reputation of the Federal and Provincial

[13] Section 37(2): "The Authority shall, with the approval of the Federal Government, prescribe rules providing for, among other matters, safeguards, transparent process and effective oversight mechanism for exercise of powers under subsection (1)."

[14] Fazal Karim, "Judicial Review of Public Actions: a treatise on judicial review, with some important background topics such as concept of jurisdiction, constitutional concept of judicial power, legislative power and executive power," Second Edition, *Pakistan Law House*, 2018.

[15] Romesh Thapper v. State of Madras (1960) SCR 594.

Government with the integrity, security and defence of Pakistan. It is submitted that such draconian provisions are reminiscent of colonial times, where laws were made with the intent to establish control over the population rather than to govern. By extending the purview of the Rules beyond the limitations legislated under the parent Act, the legislative authority of the Parliament has been overridden by the unelected Authority to infringe on the fundamental rights of citizens.

Rule 5 - Filing of Complaints:

Rule 5 states that a complaint can be filed by any person or their guardian (in cases where complainant is a minor), ministry, division, attached department, subordinate office, provincial or local department or office, law enforcement agency or intelligence agency, or a company owned by the government. Under Rule 5 (5), the identity of the complainant and the reported content shall remain "confidential." Furthermore, Rule 5 (6) gives power to the Authority to take cognizance of an unlawful online content on its own motion and pass appropriate orders.

- **Analysis:**

The word 'Complainant,' as it appears in Rule 5 and defined under Rule 3 (iii), is newly introduced by these Rules and no such expression has been used in PECA. It is also submitted that the suo-motu powers granted to PTA under Rule 5 (6) exceed the scope of PECA. PTA's powers to take cognizance of unlawful online content on its own motion can only be derived from section 37 of PECA if the said section is read in isolation.

It is an established principle of statutory interpretation that a holistic approach has to be taken and a statute must be read as an organic whole to attain consistency. As observed by Chief Justice Muhammad Munir in the case of 'Reference by President of Pakistan under Article 162,' *"the intention of the legislature in enacting a statute ought to be derived from a consideration of the whole enactment in order to arrive at a consistent plan.*[16]*"* When PECA is read in its entirety, it becomes clear that

[16] PLD 1957 SC 219.

PTA can only exercise its power to remove or block online content upon receipt of an application from an aggrieved person to remove or block a particular piece of online content. Reference is made to section 16(2), section 20(2), section 21(3), section 22(2) and section 24(3) of PECA - all of which have used the following language: *"any aggrieved person or his guardian, where such person is a minor, may apply to the Authority for removal, destruction of or blocking access to such information … and the Authority,* ***on receipt of such application****, shall forthwith pass such orders…"* While the PTA has limited powers to remove or block online content however, this power can only be exercised and is contingent upon receipt of an application from an aggrieved person or his guardian. Therefore, powers given to PTA to take cognizance of unlawful online content on its own motion cannot be inferred from section 37 of PECA. In light of the above discussion, it is reiterated that the suo-motu powers granted to PTA under Rule 5 (6) contravene and exceed the scope of PECA.

Rule 6 - Disposal of Complaints and **Rule 7 - Obligations with respect to blocking and removal of Unlawful Online content:**

Rule 6 obligates the PTA to decide complaints received by complainants within thirty days and to provide reasons in writing for its decision. It also requires the PTA to provide an opportunity of hearing to the complainant before deciding on a complaint and any such person who will be adversely affected by the decision. Further, the Rules obligate a Social Media Company, Service Provider, owner of information system/internet website/web server and User to comply with the decision of the PTA, on removal or blocking of Online Content, within twenty-four hours, and in emergency situations within six hours, from the time of receiving of the directions. Failure to comply with the directions of the PTA within the specified time will lead to initiation of action under PECA (Rule 6 (5)).

Rule 6 (6) gives powers to the PTA to require Service Provider, Social Media Company, owner of information system/internet website/web server and User to retain information, including traffic data, for such period as the PTA may specify.

Rule 7 reiterates the obligation of a Social Media Company, Service Provider, owner of information system/internet website/web server and User to comply with the decision of the Authority, on removal or blocking of Online Content, within twenty-four hours, and in emergency situations within six hours, from the time of receiving of the directions.

- **Analysis:**

It is submitted that this Rule grants unprecedented censorship powers to the PTA which has the sole discretion to determine what constitutes 'objectionable' content. The time limit of twenty-four hour is insufficient as it does not allow intermediaries to analyse the take-down request or seek any further judicial remedy. This will have a chilling effect on the content removal process as social media companies will rush content regulation decisions to comply with the restrictive time limit, leading to hasty decisions on particularly complicated cases of free speech that require deliberation and legal opinions. Given the massive volume of content shared online, platforms may feel obliged to take a 'better safe than sorry' approach--which in this case would mean 'take downfirst, ask questions later (or never).' It is also unclear whether the twenty-four hour time-limit would be put on hold in case a social media company or service provider decides to contest PTA's decision for removal of content or would the social media company be required to comply with the decision first and contest later. This threatens not only to impede legitimate operation of (and innovation in) services, but also to incentivize the removal of legitimate content. Furthermore, smaller social media companies, which do not have the resources and automated regulation capacities that big tech companies such as Facebook or Google possess, will be disproportionately burdened with urgent content removal instructions.

The Rules do not define what constitutes "emergency" cases, leaving it at the discretion of the PTA. In situations of an emergency, such as sexually explicit content causing harm on the basis of a protected category or hate speech inciting violence against an individual or community, it may be tenable to impose certain median timelines, but for content that relates to private disputes/wrongs and has a free speech element, such as defamation, it would be unreasonable to impose such a strict timeline for intermediaries to act. In all instances, the provision should

also contain “Stop the Clock” provisions by listing out a set of criteria (such as seeking clarifications, technical infeasibility, etc.) under which the time limit would cease to apply to allow for due process and fair play in enforcing such requests.

Rule 6 (5) gives powers the PTA to initiate action under PECA against information system/internet website/web server and User for failure to remove or block content hosted on its system. This provision violates the fundamental principle of intermediary liability which protects platforms and service providers from being held liable for content hosted on their platform. This principle is also preserved under section 38 of PECA which states “*No service provider shall be subject to any civil or criminal liability, unless it is established that the service provider had specific actual knowledge and willful intent to proactively and positively participate, and not merely through omission or failure to act*.” The twenty-four and six hour time frames are not sufficient for platforms to review content and failure to comply within such restrictive conditions is not sufficient justification to establish ‘willful intent’ on their part to ‘proactively and positively participate’ in offences under PECA. This provision has the effect of rendering the intermediary liability protections under section 38 of PECA meaningless.

Rule 8 - Blocking of Online System:

Rule 8 gives powers to the Authority to block "entire Online Systems or any services provided by the service providers" in case a Social Media Company, Service Provider, owner of information system/internet website/web server and User fails to abide by the provisions of these Rules.

- **Analysis:**

The manner in which section 37 of PECA is being interpreted and used by the PTA is the result of gross and erroneous misreading of the said section. While it is widely assumed that the power to block entire Online Systems is granted under section 37, a close reading clearly shows that it only grants limited powers to remove or block a particular ‘Information from the Information System’. Section 37 states, “*The Authority shall have the power to remove or block or issue directions for removal or blocking of access to* ***an*** *information through any information system*….” As evident,

limited powers to remove or block access to only a particular information have been granted as opposed to the generally understood powers to block entire Online Systems, platforms and applications. Therefore, the authority granted to PTA under Rule 8 to block entire Online Systems goes beyond the scope of section 37 of PECA and is ultra-vires the enabling Act.

Without conceding that the mandate given under section 37 of PECA allows blocking of entire Online Systems, it is still submitted that the power to 'block' an Online System is a violation of Article 19 of the Constitution as well. The said Article only allows 'reasonable restrictions' to be imposed on free expression in accordance with law. It was held in Civil Aviation Authority Case[17] that "*the predominant meanings of the said words (restrict and restriction)* ***do not admit total prohibition****. They connote the imposition of limitations of the bounds within which one can act*..." Therefore, the power to 'block' cannot be read under, inferred from or assumed to be a part of the power to restrict free speech. While Article 19 of the Constitution allows imposition of 'restrictions' on free speech, the power to 'block' an information system entirely exceeds the boundaries of permissible limitations under it and renders Rule 8 inconsistent with the Constitution.

It is submitted that in today's digital world, Online Systems allow individuals to obtain information, form, express and exchange ideas and are mediums through which people express their speech. Hence, entirely blocking an Online System is synonymous with blocking speech itself. The blocking of Online Systems, as a blunt instrument will cause unintended consequences, including preventing Pakistani citizens and companies from benefiting from access to resources from the rest of the world, thus inhibiting the country and reinforcing a digital divide.

Rule 9 - Other Obligations of the Service Providers and Social Media Companies:

Under Rule 9, Social Media Companies and Service Providers have been directed to issue Community Guidelines for usage of their respective platforms. Adding on to it,

[17] PLD 1997 SC 781.

Rule 9 (2) states that these guidelines should inform the users not to transmit, display or disseminate Online Content that:

A. Belongs to another person and to which the User does not have any right,
B. Is blasphemous, defamatory, obscene, pornographic, pedophilic, invasive of another's privacy
C. Violates or affects religious, cultural, ethnic sensitivities of Pakistan
D. Harms minors in any way
E. Impersonates another person
F. Threatens the integrity, security or defence of Pakistan.

Rule 9 (3) requires Social Media Companies and Service Providers to deploy appropriate mechanisms to identify Online Content that needs to be blocked / removed under the Rules. Under Rule 9 (4), Social Media Companies and Service Providers are prohibited from displaying, hosting, uploading or publishing any Online Content barred under the Rules.

Furthermore, Rule 9 (5) directs Social Media Companies and Service Providers with over 500,000 users to register with the Authority, establish a permanent registered office in Pakistan and appoint a focal person based in Pakistan within nine months of coming into force of these Rules. Rule 9 (5) also obligates Social Media Companies and Service Providers to establish one or more database servers in Pakistan and Rule 9 (7) requires them to provide "decrypted readable and comprehensible information" to the Federal Investigation Agency in accordance with the provisions of PECA.

Rule 9 (9) provides that Social Media Companies and Service Providers shall deploy mechanisms to ensure prevention of uploading and live streaming of Online Content regarding terrorism, extremism, hate speech, pornographic, incitement to violence and detrimental to national security.

Under Rule 9 (10), the Authority is empowered to impose a penalty of up to PKR 500 million on Service Providers and Social Media Companies in case they fail to abide by the Rules or PECA or any direction passed by the Authority in pursuance of these Rules.

- **Analysis:**

Mandating social media companies to develop Community Guidelines in line with the Rules essentially has the effect of privatising censorship by asking companies to enforce restrictive speech practices. Secondly, by developing separate content moderation and community guidelines for Pakistani citizens, the Rules will result in a fundamentally different internet for Pakistan as opposed to the rest of the world.

Rule 9 (9) obligates a social media company to deploy proactive mechanisms to ensure prevention of live streaming of any content with regards to, amongst other things, '*hate speech*' and *'extremism.'* It should be noted that determination of both these offences require a thorough investigation and a trial. If a trial and investigation is necessary to determine these offences then it would be nearly impossible for social media companies to deploy mechanisms to prevent their live streaming. Even otherwise, hate speech is an entirely contextual determination, where the illegality of material is dependent on its impact. Impact on viewers is impossible for an automated system to assess, particularly before or during the material is being shared. The provisions obscure difficulties in making real-time determinations regarding live streaming of content. It is highlighted that social media companies already regulate live-streamed content and in wake of the 'Christchurch Call' measures have been introduced to tighten restrictions.

It is also noted that Rule 9 (9) is in conflict with section 38 of PECA which provides a comprehensive limitation of liability to intermediary service providers. Section 38 of PECA protects service providers from fines and imprisonment if someone uses their systems to break the law without their knowledge or participation. Despite these protections, the Rules now compel not just social media companies but also service providers to keep a proactive watch on online user activity to prevent blasphemy, cultural insensitivity, harm to minors, and threats to national security, among other issues. Section 38 (5) of PECA also expressly rejects imposition of any obligation on intermediaries or service providers to proactively monitor or filter material or content hosted, transmitted or made available on their platforms. However, the Rules effectively negate these protections.

Data Localisation:

It is submitted that the requirement for registering with PTA and establishing a permanent registered office in Pakistan, before these companies can be granted permission to be viewed and/or create content in Pakistan, is a move towards "data localisation" and challenges the borderless nature of the internet - a feature that is intrinsic to the internet itself. Even otherwise, forcing businesses to create a local presence is outside normal global business practice and compels an investment without a business need. Such a regulation will force international social media companies to exit the country rather than invest further in Pakistan.[18] It is unreasonable to expect companies to set up infrastructure in the country when the nature of the internet allows for it to be easily administered remotely. With an increase in compliance costs that comes with incorporation of a company in Pakistan, companies across the globe including start-ups may have to reconsider serving users in Pakistan. Consequently, users in Pakistan including the local private sector may not be able to avail a variety of services required for carrying out day-to-day communication, online transactions, and trade/business related tasks. The proposed Rules requiring local incorporation and physical offices will also have huge repercussions on taxation, foreign direct investment and other legal perspectives along with negatively impacting economic growth.

Rule 9 further requires social media companies to establish database servers in Pakistan to record and store data and online content. This provision is alarming inasmuch as it threatens the state of privacy of citizens in Pakistan because there are no data protection laws within the country at the moment[19] - leaving the data/information so collected or gathered to open abuse and misuse.

To effectively defend against cybercrimes and threats, companies protect user data and other critical information via a very small network of highly secure regional and

[18] Major tech companies have already expressed their reservations with the Rules and the possibility of exiting the country:
https://aicasia.org/2020/11/20/pakistan-aic-issues-media-statement-on-removal-and-blocking-of-unlawful-content-procedure-oversight-and-safeguards-rules-20-nov-2020/.

[19] DRF and other civil society organisations have expressed reservations with the current draft of the Personal Data Protection Bill:
https://digitalrightsfoundation.pk/wp-content/uploads/2020/05/PDPB-2020_-Final-Analysis_05.05.2020-1.pdf

global data centers staffed with uniquely skilled experts who are in scarce supply globally. These centers are equipped with advanced IT infrastructure that provides reliable and secure round-the-clock service. The clustering of highly-qualified staff and advanced equipment is a critical factor in the ability of institutions to safeguard data from increasingly sophisticated cyber-attacks.

Mandating the creation of a local data center will harm cybersecurity in Pakistan by:

- Creating additional entry points into IT systems for cyber criminals.
- Reducing the quality of cybersecurity in all facilities around the world by spreading cybersecurity resources (both people and systems) too thin.
- Forcing companies to disconnect systems and/or reduce services.
- Fragmenting the internet and impeding global coordination of cyber defense activities, which can only be achieved efficiently and at scale when and where the free flow of data is guaranteed.

Preventing the free flow of data:

- Creates artificial barriers to information-sharing and hinders global communication;
- Makes connectivity less affordable for people and businesses at a time when reducing connectivity costs is essential to expanding economic opportunity in Pakistan, boosting the digital economy and creating additional wealth;
- Undermines the viability and dependability of cloud-based services in a range of business sectors that are essential for a modern digital economy; and
- Slows GDP growth, stifles innovation, and lowers the quality of services available to domestic consumers and businesses.

Requiring local incorporation and presence unnecessarily discriminates against foreign businesses, poses a non-tariff barrier to trade, and unfairly tilts the playing field in favour of domestic players. This is particularly stark in view of the nature of the services provided through the internet, which can be provided on a cross-border basis without the need for physical presence. By instituting local presence requirements, Pakistan is deviating from established international trade norms and practices, and erecting unnecessary barriers to cross-border services trade.

The global nature of the internet has democratized information which is available to anyone, anywhere around the world in an infinite variety of forms. The economies of scale achieved through globally located infrastructure have contributed to the affordability of services on the internet, where several prominent services are available for free. Companies are able to provide these services to users even in markets that may not be financially sustainable as they don't have to incur additional cost of setting-up and running local offices and legal entities in each country where they offer services. Therefore, these Rules will harm consumer experience on the open internet, increasing costs to an extent that offering services/technologies to consumers in Pakistan becomes financially unviable.

Privacy:

Rule 9 (7) requires social media companies to provide "decrypted, readable and comprehensible information" to the Federal Investigation Agency (hereinafter as the "**FIA"**). This provision essentially amounts to a key disclosure law or mandatory key disclosure law, in that it requires social media companies, platforms and service providers to hand over encrypted data to law enforcement. While the FIA can send data requests to companies in order to investigate crimes under PECA, the requirement for data to be decrypted threatens the privacy expectation of users on encrypted platforms. Furthermore, often platforms do not have access to encryption keys themselves to effectively decrypt data and information. On the other hand, requiring companies to develop backdoors to encryption will expose entire platforms and services to attacks, thus undermining the overall privacy of all users. Instead of focusing on a rights-compliant data sharing mechanism that respects the privacy of users and focuses on timely retrieval of data for the most heinous of crimes, these Rules replicate the worst international practices focused on control of data rather than genuine issues faced by citizens.

Rule 11: Review and **Rule 12: Appeal**

Under Rule 11, any person aggrieved by any order or direction of the PTA under the Rules may file a review application within thirty days from the date of the passing of

the order, and it will be decided within thirty working days. As per Rule 12, an appeal against the decision of the Authority in review can be filed in a high court within thirty days of the order of the authority.

- **Analysis:**

It is submitted that the remedy for review and appeal provided under the Rules are very limited and narrow. The appeal will be against the review order of the PTA and not against the original order of the Authority. This essentially means that the jurisdiction of the High Court while hearing the appeal will be limited to adjudication upon the grounds of the review and not the entirety of the record. This limited appeal is, therefore, largely ornamental as it leaves the citizens whose fundamental rights have been infringed without an efficacious right of appeal.

Rule 16: Public Education and Awareness

Rule 16 instructs the Authority to take measures for awareness of the general public on matters relating to removal and blocking of unlawful Online Content over the internet within thirty days of the publication of these Rules.

- **Analysis:**

The document published by the Ministry states that the Rules were published on 20 October, 2020 and were only made public on 18 November, 2020. The thirty day period since publication has already lapsed and the PTA has made no efforts to educate the public at large regarding the impact of these Rules on citizens' online free speech. The entire publication of the Rules has been shrouded in mystery despite repeated requests by industry and civil society actors to make the rules public earlier.

Concluding Remarks

We reiterate that section 37 of PECA in its present form is unconstitutional and unacceptable on grounds of freedom of expression. A regulation formulated in furtherance of an unconstitutional provision is also doomed to fail. We remind the government that its cardinal duty is to uphold and strengthen democratic values and protect human rights and civil liberties. However, these Rules, which are wholly undemocratic, threaten and undermine our fundamental rights to free expression and privacy. In light of these violations and the concerns we have raised in this analysis, DRF demands that these Rules be immediately de-notified. We also call upon the government to amend the draconian PECA with a complete repeal of its section 37. Any future regulations on social media and internet control should ensure that government policy does not invalidate our digital rights.