DigitalRightsFoundation
"KNOW YOUR RIGHTS"

Citizens Protection (Against Online Harm) Rules, 2020: Legal Analysis

The 'Citizens Protection (Against Online Harm) Rules, 2020' have been notified under sections of the Pakistan Telecommunication (Re-organisation) Act, 1996 and the Prevention of Electronic Crimes Act (PECA) 2016 (hereinafter collectively referred to as the '**Parent Acts**'). Under these Rules, the Pakistan Telecommunication Authority is the designated Authority. This legal analysis will highlight the jurisdictional and substantive issues with the Regulations in light of constitutional principles and precedent as well as larger policy questions.

Summary of the Legal Analysis

Given that the Rules exceed the scope of the Parent Acts and substantively violate the fundamental/Constitutional rights, particularly Article 14 and 19, they are inconsistent and in derogation with the Constitution as well as the Parent Acts and should be immediately denotified.

Rule	**Analysis**
Rule 3: Establishment of National Coordinator	Establishment of National Coordinator goes beyond the scope of the Parent Acts in the creation of the the National Coordinator. The power granted under PECA and PT (Re-organisation) Act to make 'Rules' does not include the power to make an entirely new body i.e. National Coordinator. Moreover, there is no prescribed qualification or criteria for selection and appointment of the proposed National Coordinator who has been given vast and discretionary powers.
Rule 4: Obligations on Social Media Company with respect to blocking and removal of unlawful online content	Exceeds the boundaries of permissible restrictions within the meaning of free speech under Article 19. Lacks the necessary attributes of reasonableness inasmuch as no safeguards are provided under the Rules against arbitrary exercise of power. Restriction on speech can only be imposed in accordance with 'law,' and the 'instructions' of National Coordinator cannot be deemed to be Law. Even otherwise, the 'instructions; have no defined scope and are too arbitrary to curtail fundamental rights.

Rule 5: Other Obligations of the Social Media Companies.	Establishing database servers in Pakistan to record and store data and Online Content threatens the state of privacy of citizens in Pakistan because there are no Data protection laws within the country - leaving the Data/information so collected or gathered to open abuse and misuse. The requirement for data localisation has the potential to be an economic disincentive for companies to invest in Pakistan and deny Pakistani citizens access to platforms.
Rule 6: Provision of information by Social Media Company	Lack of legal or judicial procedures/safeguards to make a request requiring information. The Rules do not distinguish between traffic and content data, casting a wide net in terms of information that can be procured.
Rule 7: Blocking of Online System	The power to block entire Online Systems/Platforms cannot be delegated to the National Coordinator and to do so would be exceeding the scope of the Parent Acts. PECA provides the power to block a particular information from an information system whereas this rule grants power to block entire Online System. Hence, it goes beyond the scope of PECA.

Detailed Legal Analysis

Scope and Jurisdiction

The additional powers of the Rules go beyond the scope of the Parent Acts, i.e. Pakistan Telecommunication (Re-organization) Act, 1996 and the Prevention of Electronic Crimes Act, 2016.

Requirements such as local incorporation and data localization are beyond the scope of powers conferred under Section 51 of PECA. In fact, the scope and definition of service providers under Section 2 (xxviii) of PECA do not envisage any such limitations.

Further, PECA specifically proscribes any obligation on service providers to proactively monitor or filter live streaming content on their platforms. On the contrary, these Rules impose extremely onerous obligations on service providers to identify and remove all 'unlawful content' from their platforms. The imposition of such pre-conditions on service providers are entirely contrary to the spirit of Section 38 PECA which provides immunity to service providers qua UGC content on their platforms. Notably, the proposed Rules even empower the National Coordinator to block entire platforms of service providers for any non-compliance with the Rules.

Rule 3: Establishment of the National Coordinator

Rule 3 establishes the office of a National Coordinator in an attempt to centralise the control of online regulation to this office. The Rules instruct the Information Technology and Telecommunication minister to designate the National Coordinator within fifteen days of its notification. It will be responsible for coordinating with stakeholders for regulating Online Systems – a term which includes all Social Medial Applications, Over the Top Applications (applications for messaging, voice and video calls like WhatsApp, Facebook Messenger, Viber, Skype, etc.) and any cloud-based content distribution services. The National Coordinator shall also issue instructions related to blocking of unlawful online content and acquisition of data or information from social media companies. Finally, the National Coordinator is empowered to engage with social media companies on behalf of the federal government and direct the official representatives of any Social Media Company to appear before it.

Analysis

Protecting online security is an important priority; however, the ambiguously defined scope, vague language and lack of safeguards in the Rules raises serious privacy concerns for both individuals and businesses. There are no prescribed qualifications and criteria for selection and appointment of the proposed National Coordinator. This is especially concerning considering the extensive powers of the National Coordinator, including quasi-judicial and legislative powers to determine what constitutes a harm.

Provisions that allow the Office of the National Coordinator to search and seize data without proper legal oversight are particularly concerning. This would give the regime sweeping powers to monitor online traffic in the name of an emergency or as a preventive measure, potentially compromising private and corporate data. This is contrary to the scheme of PECA, 2016 under which only PTA may seek removal of unlawful online content and agencies authorised under Section 29 PECA may seek user data. Further, the Rules do not formulate sufficient safeguards to ensure that the power extended to the National Coordinator is used by government agencies in a fair, just, and transparent manner.

Rule 4: Content removal by social media companies

Rule 4 obligates a Social Media Company to remove, suspend or disable access to any Online Content within twenty-four hours, and in emergency situations within six hours, after being intimated by the Authority that any particular Online Content is in contravention of any provision of the Act, or any other law, rule, regulation or instruction of the National Coordinator.

Analysis

It is submitted that Rule 4 is a blatant violation of Article 19 (freedom of speech, etc.) of the Constitution. It exceeds the boundaries of permissible restrictions within the meaning of Article 19, lacks the necessary attributes of reasonableness and is extremely vague in nature.

While Article 19 of the Constitution of Pakistan has laid down the purposes for which a restriction on speech may be placed, the Rules require all Social Media companies to remove or block Online Content if it is, among other things, in "*contravention of instructions of the National Coordinator."* The criteria laid down is extremely vague and open to arbitrariness. The Rules fail to provide any checks and balances to ensure that such requests are used in a just manner. It is to be noted that contravening the instructions of the National Coordinator is not a not a purpose for which a restriction on freedom of speech may be placed under Article 19. Moreover, a restriction on freedom of speech may only be placed in accordance with law and an instruction passed by the National Coordinator cannot be deemed as law.

On interpretation or permissibility of any online content, as per Rule 4 (2), the opinion of the National Coordinator is to take precedence over any community standards and rules or guidelines devised by the Social Media Company. It is trite law that a restriction on freedom of speech will be unreasonable if the law imposing the restriction has not provided any safeguards against arbitrary exercise of power (PLD 1964 SC 673). However, Rule 4 (2) encourages arbitrary and random acts and bestows upon the National Coordinator unfettered discretion to regulate online content instead of even remotely attempting to provide any safeguards against abuse of power.

The time limit of 24 hours is insufficient as it does not allow intermediaries to analyse the take-down request or seek any further judicial remedy. In situations of an emergency, 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 4 (4) requires Social Media Companies to deploy proactive mechanisms to ensure prevention of live streaming through online systems particularly regarding Online Content related to terrorism, extremism, hate speech, defamation, fake news, incitement to violence and national security. A fundamental flaw within this Rule is the vague, overly broad and extremely subjective definition of "extremism." It is defined as '*violent, vocal or active opposition to fundamental*

values of the state of Pakistan including…" It does not, however, define what constitutes or can be referred to as fundamental *values* of the state Pakistan. 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 down first, ask questions later (or never).' These threaten not only to impede legitimate operation of (and innovation in) services, but also to incentivize the removal of legitimate content. This is one of the reasons why laws and policy principles have generally not required platforms to proactively monitor and filter all content.

Moreover, an honest criticism or a fair comment made regarding the Federal Government, or any other state institution, runs the risk of being seen as 'opposition,' as this word also lacks clarity. Similarly, while a Social Media Company is required to prevent 'fake news,' the Rules do not expound on this word - adding further to the ambiguity of the Rules. It is noted that fake news laws across the world have been criticised from a free speech perspective, and strengthening of fact-checking institutions is a more rights-compliant way to tackle free speech online. It must also be noted that a key precondition to a fair trial is that criminal offences must be formulated clearly and precisely to ensure individuals can regulate their conduct accordingly. Vague laws weaken the rule of law because they enable selective prosecution and interpretation, and arbitrary decision-making. It is trite law that "*the language of the statute, and, in particular, a statute creating an offence, must be precise, definite and sufficiently objective so as to guard against an arbitrary and capricious action on part of the state functionaries...*"

It must also be pointed out that this provision goes beyond the scope of laws under which the Rules are ostensibly made, such as Pakistan Telecommunication (Reorganization) Act, 1996 and PECA-2016 - none of which contain a provision as to the dissemination of 'fake news.'

Rule 5: Localisation

Rule 5 obligates Social Media Companies to register with the Authority within three months of coming into force of these Rules. It requires a Social Media Company to establish a permanent registered office in Pakistan with a physical address located in Islamabad and to appoint a focal person based in Pakistan for coordination with the National Coordinator.

Analysis

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. It is unreasonable to expect from them 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 come 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 a huge repercussion on taxation, foreign direct investment and other legal perspectives along with negatively impacting economic growth.

Rule 5 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 - 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 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, increase costs to an extent that offering services/technologies to consumers in Pakistan becomes financially unviable.

Finally, Rule 5 obligates Social Media Companies to put a note along-with any Online Content that is considered or interpreted to be 'false' by the National Coordinator. Not only does this provision add to the unfettered powers of the National Coordinator to be exercised arbitrarily but also makes the Coordinator in-charge of policing truth. This violates the principles of freely forming an 'opinion' (a right read as part of Article 19) as the National Coordinator now decides, or dictates, what is true and what is false. It also goes beyond the scope of PECA and PTA (Re-organisation) Act - none of which contain a provision as to the determination of falsehood.

Rule 6: Provision of Information by Social Media Companies

Rule 6 requires a Social Media Company to provide to the Investigation Agency *any* information, data, content or sub-content contained in any information system owned, managed or run by the respective Social Media Company. Given the current PECA regulations, there is still a legal process through which information or data of private users can be requested. This Rule, however, totally negates the current process.

Analysis

Astonishingly, the agency is not required to go through any legal or judicial procedure to make such a request and it is not even required to notify or report to a court on seizure of any such information. This gives total control to the Investigating Agency over content not just being shared on public digital platforms but also on content being exchanged through private communication networks. It violates the principles of privacy as enshrined in the Constitution of Pakistan. The Rule does not distinguish between traffic and content data, casting a wide net in terms of information that can be procured. It is standard practice to have higher protections for content data as citizens have a reasonable expectation of privacy that the contents of their

conversations and communications will not be surveilled. The requirement to provide information in "decrypted, readable and comprehensible format" is unprecedented and violates the basic privacy rights of citizens.

Rule 7: Blocking of online system

Rule 7 grants power to the National Coordinator to block the entire Online System, Social Media Application or services owned or managed by a Social Media Company or to impose a penalty of five hundred million rupees in case a Company fails to abide by the provisions of these Rules.

Analysis

The power to 'block' an entire Online System is a violation of Article 19 of the Constitution which provides the power to impose reasonable 'restrictions' on free speech, is over-broad and a disproportionate measure denying access of citizens to entire platforms. In today's digital world, Online Systems - which are defined under the Rules as Social Media applications, OTTAs and any cloud-based content distribution services, allows individuals to form, express and exchange ideas and are mediums through which people obtain their information on political matters. Hence, entirely blocking an Online System would be tantamount to blocking speech itself.

It must also be noted that the power to 'entirely block' cannot be read under, inferred from, or assumed to be a part of the power to 'restrict' free speech. It was held, in Civil Aviation Authority Case (PLD 1997 SC 781), 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…*" Any sanction should focus on systemic failures to abide by the rules, rather than detailed specific one-off elements. Companies should also be given notice and an opportunity to appeal, explain their approach, and when actually necessary, rectify alleged failures. Therefore, while Article 19 allows imposition of 'restrictions' on free speech, the power to 'entirely block' exceeds the boundaries of permissible limitations under it – rendering Rule 7 inconsistent with the Constitution.

The blocking of online systems, as a blunt instrument that will cause unintended consequences, including to prevent 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. It must also be noted that the power to 'block' entire Online Systems is going beyond the scope of PECA which grants, inter-alia, the power only to block a particular 'information' from an information system and not the power to block an entire Online System. Evenotherwise, the power to block, which is derived from PECA, cannot be delegated to the National Coordinator as no provision of delegation of powers is given under PECA.