International Journal of Human and Society (IJHS)

P-ISSN: 2710-4966	E-ISSN: 2710-4958
Vol. 4. No. 01 (Jan-Mar) 2024	Page 1360-1370

Cyber Laws In Pakistan: Bridging The Gap Between National And International Standards

Dr. Adeel Abid	A Ph.D. lawyer and Associate Professor at DIHE, enrolled in the Supreme Court of Pakistan and Partner in the LAW Firm M/S. Surridge & Beecheno adeel77abid@yahoo.com
Zeeshan Hyder	L.L.B.- University of London and Associated with the LAW Firm M/S. Surridge & Beecheno aleezeeshan502@gmail.com
Arbab Zalland Kasi	LLB. University of London and a practicing Lawyer, Associated with the LAW Firm M/S. Surridge & Beecheno arbabzallandkasi@gmail.com

Abstract: *The concept of law has always been considered a social institution, serving as a responsive mechanism to address evolving social exigencies. This foundational principle finds resonance in the renowned proclamation of an esteemed American jurist who articulated, "I am content to conceive of law as a social institution designed to fulfill societal exigencies..." (Introduction to the Philosophy of Law). In contemporary times, as humanity witnesses unprecedented technological innovations and advancements, while these developments undoubtedly enhance human convenience, they also engender profound concerns regarding data security and privacy infringement. Concurrently, in the face of burgeoning challenges such as climate change and the complexities posed by artificial intelligence, the peril of cyber-attacks emerges as a formidable threat that demands heightened attention from governmental bodies and international entities alike. Hence, it behooves states to recognize cyber-attacks as a pivotal concern meriting substantial regulatory and strategic responses to safeguard the integrity of digital infrastructures and preserve individual privacy rights amidst the escalating digital landscape.*

The paper provides an overview of the current status of cyber laws in Pakistan and their enforcement mechanisms. It highlights key legislative frameworks such as the Federal Investigation Agency Act and the Prevention of Electronic Crimes Act, along with their strengths and weaknesses in addressing cybercrimes. The paper also compares Pakistan's legal landscape with that of the United States and the European Union, noting disparities in development and implementation. It emphasizes that in a country like Pakistan, where a concerning number of laws are archaic and outdated, a decent overhaul of the existing laws is necessary to protect citizens' privacy and data. By the end of the study, the paper aims accentuate the potential flaws in the Pakistani cyber law framework and attempt to do a comparative analysis with more developed countries such as the United States and certain European countries.

Keywords: Cybersecurity, Federal Investigation Agency, cybercrimes, Surveillance, Right to Privacy

SCOPE OF STUDY:

In the instant paper following questions will be addressed:

1. How do the divergent jurisprudential frameworks of cyber laws in Pakistan, the United States, and the European Union entail as regards cyber security measures and individual rights in each of those countries?

2. How does the Federal Investigation Agency (FIA) function within Pakistan's cybercrime complaint handling system, and what obstacles are encountered during this process?

3. How does the Prevention of Electronic Crimes Act (PECA) contribute to cybersecurity assurance and whether there is a need for reform in the act?

HISTORICAL CONTEXT:

The world was first introduced to general purpose computers in 1946, with the invention of ENIAC. Initially the scope of the technology was limited due to their extreme bulkiness and high costs. However, its convenience and usefulness became eminent with time and technological advances. In the present day, the computers are used for almost everything ranging from the defense industry (aircrafts and missile systems etc.) to medical, entertainment and banking industries. Due to how fast computers have become part of the daily lives, it is hard reconcile the fact that the first general purpose computer was invented only 75 years ago. Nonetheless, there is always a segment of society which tends to misuse technology for selfish gain while causing detriment to another. That segment became prominent as early as 1940 when Rene Carmille became the first ethical hacker who allowed the Nazi's to use his tracking machine to track Jews while he was hacking the machine and disrupting their efforts (Monroe College, 2024). Decades later, in order to combat and avoid potential ethical hackers a programmer named Bob Thomas, in 1971 created and deployed a virus that served as a security test used to highlight potential security flaws and vulnerability in the system, which is believed to have been the very first attempt at cybersecurity (Monroe College, 2024). Due to the advent of a new form of technology, and a gradual surge in crimes associated thereof, a new term was coined; 'Cybercrimes'. Defined as a crime which is committed on the internet or some computer with the help of a software in order to destroy another computer or to gain information by way of stealing and hacking data). Also termed as computer crime in certain places (Razi, N., & Zahoor, R). Cyber security, therefore, is a broad term which includes cyber-attacks on the nation as a whole (i.e. national security threats) and misuse and misappropriation of personal data of individuals.

CURRENT STATUS OF CYBER LAWS IN PAKISTAN & THEIR ENFORCEMENT:

The Constitution of Pakistan doesn't explicitly mention cybercrimes or prohibit the practice, instead the constitution guarantees rights in a general manner, such as the right to Inviolability of dignity of man covered by article 14 of the constitution (Constitution of Islamic Republic of Pakistan. (1973). Like most other jurisdictions, the cybercrimes are regulated by Acts enacted with constitutional force and authority. These include the FIA Act, the Prevention of Electronic Crimes Act (PECA) etc. Pakistan is also a signatory of numerous international conventions which aim to safeguard the right to privacy and security. These include the Universal Declaration on Human Rights (United Nations General Assembly. (1948)., the Convention on the rights of the Child (United Nations General Assembly. (1989)., the Cairo Declaration on Human Rights in Islam etc.

I. FEDERAL INVESTIGATION AGENCY ACT, 1974

An example of one of the legislations Pakistan has enacted to regulate the cyberspace and crimes associated thereof is the Federal Investigation Agency Act, 1974. The act establishes the Federal Investigation Agency as a key department for investigation of crimes associated with computers, internet and illegal use of information technology etc. The organization has also been empowered to initiate legal actions under extra-territorial jurisdiction in criminal matters. The cross border mandate of the FIA under the law is vested due to its ability to coordinate and have a direct liaison with the INTERPOL.

However, despite having extensive power, there are certain concerns which are believed to be responsible for hampering the organization. One such problem pertains to the complaint lodging process with the FIA cybercrime cell. It is known to be a lengthy and time-consuming process as it involves several steps to ensure proper documentation and investigation. Firstly,

individuals have to physically visit the FIA cybercrime cell to lodge their complaint. Though, they can contact the FIA via email or call the helpline number (9911), it is essential for the complainant to visit the FIA at least once for confirmation purposes. (Jamshed, J., & W. R. 2022)

Secondly, due to it being an extremely slow process, many individuals approach the FIA only when they have exhausted all other means, leading to delays in the initiation of the formal complaint procedure. It typically takes between 30 to 60 days to commence the proper investigation process for any complaint. Moreover, the time taken for identification varies, ranging from the same day to up to a month. (Jamshed, J., & W. R. 2022)

The third reason why this avenue is not a popular choice for redressal is the sheer lack of awareness pertaining to the procedure and its efficacy. The general public believes FIA to only be an organization which gets involved when cybercrimes or inter-state crimes occur but they are unaware of the fact that an individual can lodge a complaint with the organization to seek proper redressal. Lack of awareness coupled with public distrust forms a bad amalgam leading the institution to become far less effective than it should be. The public distrust could also stem from the renowned incompetence of the Pakistani Police, regardless, they fact remains, it is an un-popular choice mostly.

II. PREVENTION OF ELECTRONIC CRIMES ACT, 2016:

The prevention of Electronic Crimes Act, 2016 (PECA) is comprehensive piece of legislation enacted by the National Assembly to regulate the electronic crimes and provide a mechanism for investigation, prosecution, and adjudication in relation to electronic crimes. (Majid, A., Haider, I., Babr, K., & Saad, M. (2018). In previous enactments, the number of offences was limited. To address this issue, many offences such as illegal access of data (hacking), DOS and DDOS attacks, electronic forgery and electronic fraud and cyber terrorism were also included in the PECA. The legislation provides new investigative powers which were unavailable before such as search and seizure of digital forensic evidence using technological means, production orders for electronic evidence, electronic evidence preservation order, partial disclosure of traffic data, and real time collection of data under certain circumstances and other enabling powers which are necessary to effectively investigate cybercrime cases.

While the inclusiveness of the Act is commendable, PECA is not without its flaws. First and most importantly, the Act has been framed in a way that it contradicts the inalienable guarantee of privacy and security provisions provided in the Constitution. In particular, section 31 of the Act is clearly contradictory to the right to privacy and data protection. It allows the authorized agent to hand over personal data without the prior court warrant where it believes that the impugned information is "reasonably" required (Khan, E. A.). The ambiguity of the word 'reasonable' has caused concerns surrounding arbitrary violations of privacy and personal space. Section 31 of the act, therefore, can be used to transfer personal data and information arbitrarily without any restriction due to the free reign the wording of the act has provided to the authorities. Such unfettered discretion not only undermines the fundamental right to privacy but also jeopardizes the integrity of data protection measures. Whilst it is a violation of privacy for a good amount of people, it is also plausible that in certain situations the discretion is required in order to make the process and investigation more effective. Consequently, it is imperative that we advocate for the revision of Section 31 to be worded in a way to safeguard the sanctity of privacy rights and fortify the framework of data protection while also ensuring a good balance between protection and safety within our legal system.

Another argued flaw with the act pertains to its definition of cyber-terrorism, as critics argue that the definition has been defined too broadly. They believe that cyber-terrorism offenses must be clearly linked to "violence and the risk of harm and injury." Since Section 10(b) declares

the advancement of "inter-faith, sectarian, or ethnic hatred" as a qualifier for cyber-terrorism they believe it to be too broad. At the same time is imperative not to see the reasoning behind the legislature's actions. It is not necessarily a negative that the provision associates terrorism with violence or hostility or even hatred. The most elaborate example in this regard is Myanmar and their treatment of the Rohingya Muslims. A group of people who were expelled from Myanmar subsequently after a brutal ethnic cleansing in 2017, which unintentionally initiated using Facebook as propaganda tool to promote hatred against the Rohingya Muslims. It all spiraled out of control due to the fact that none of the Facebook directors spoke or understood the Burmese language, and there was only one Facebook employee overseeing the region. Facebook ended up promoting posts which included violence and propaganda against the Rohingya Muslims in a very elaborate way, leading to genocide (Amnesty International. 2022, September 29). Examples such as these are pertinent to protect ethnic minorities and other groups which might end up suffering due to a lack of regulation and propaganda being spread to mostly illiterate individuals.

III. INVESTIGATION FOR FAIR TRIAL ACT, 2013

The Investigation for Fair Trial Act 2013 is an act which empowers law enforcement and intelligence agencies to collect evidence by modern devices and means without there being a need for a warrant from competent authority. This gives the agencies a free reign over the populous as the act itself does not narrow down the situations where it is applicable. It can be valid for a broad range of dissimilar situations as it permits the surveillance if the nature thereof "is such that it is not necessary to serve the warrant on anyone" (Bukhari, F. H. (2014). Such unfettered discretion is being exercised till date due to the amount of power the Establishment possesses in the country. As Furhan Hussain and Gul Bukhari put it,

"according to Pakistan Telecommunication (Re-organization) (Amendments) Act, 2006, the government can authorise any person(s) to intercept calls and messages, or trace location or movement through any telecommunication medium, giving the authorities a free hand to conduct communications surveillance, and with no mention of any governance parameters ensuring a due process." (Bukhari, F. H. (2014).

Another interesting point mentioned by Bukhari & Hussain is that PTA itself has the authority to conduct communications surveillance however it denies doing so and admits that the Establishment's legal wing monitors the "grey traffic" over the internet despite lacking legal authority to do so. This is the key factor in understanding the surveillance laws in Pakistan and how such unfettered discretion being present with one organization separates it from others.

On the other hand, in the landmark case of Mohtarma Benazir Bhutto Case, (P L D 1998 Supreme Court 388) the Supreme Court declared that surveillance is not only unlawful but also immoral and a violation of constitutional rights, with no valid justifications. The Court underscored that *"The inviolability of privacy is directly linked with the dignity of man. If a man is to preserve his dignity, if he is to live with honor and reputation, his privacy whether in home or outside the home has to be saved from invasion and protected from illegal intrusion. The right conferred under Article 14 is not to any premises, home or office, but to the person, the man/woman wherever he/she may be"* (Para 30). Consequently, the Supreme Court has affirmed that telephone conversations enjoy the same level of privacy protection guaranteed by the Constitution. This landmark ruling is certainly a step in the right direction, however, it doesn't appear as though the surveillance in Pakistan has reduced as a result of this judgment specifically.

Despite there being capable organizations which can aid against cyber security threats, there have been times where Pakistan has suffered due to a failure on part of the cyber security enforcers. The most recent examples of these attacks include the attack on National Institutional Facilitation Technologies (NIFT) where, *"Cyber attackers managed to breach the security of the cheque-clearing institution, gaining unauthorised access to data and forcing*

the banking system to resort to a manual system despite the prevalence of digital technology… The NIFT issued a statement claiming that there was no "significant compromise" of its data or systems. However, the statement suggests that some level of security breach did occur, although it was considered insignificant." (Tribune.pk. July 07,2023). Similarly a month later, there was a cyber-attack on the Election Commission of Pakistan where hackers were attempting to send malicious links used to steal data via emails. In May of 2023, Deputy Permanent Representative of Pakistan to the UN, Ambassador Aamir Khan told the UN Security Council that "it would be salient to suggest that only a legally binding instrument tailored exclusively to address the specific conditions and interests of all states would be the best way forward" in response to rampant increase in cyber-attacks (Tribune.pk. July 07,2023). It is not believed that this would be the solution to this issue. It is rather more plausible to establish a new statutory legally binding authority to specifically deal with national security threats or empower and administer the existing ones (FIA) in such a way that they become well equipped for dealing with such issues.

IV. ELECTRONIC TRANSACTIONS ORDINANCE (ETO) 2002 & CERTIFICATION SERVICE PROVIDER'S ACCREDITATION REGULATIONS 2008.

Another act pertinent enough to be mentioned here is the ETO 2002, and the Certification Service Provider's Accreditation Regulation 2008 enacted later under ETO's authority. Despite it not being too revolutionary in terms of cybersecurity protection, it still brought a noteworthy change in Pakistan which cannot be ignored. Prior to the enactment of the ETO 2002, Pakistan had an inefficient Paper-based process and limited, stagnant growth in E-commerce was noticeable. Therefore in 2002 the ETO was enacted by the legislature which provided legal recognition to electronic transactions and documents. A new system of digital signatures was introduced making the processes relatively less time consuming whilst also facilitating e-commerce by formulating a more protected and trustworthy environment for it to thrive. ETO wasn't the sole factor however it is certain to have played a significant role in aiding E-commerce in Pakistan. It is not without its flaws nonetheless, the alleged key flaws include a lack of liability for the Certification Service Providers in case of fraudulent certificate issuance, lack of any consumer protection provisions within the Ordinance, lack of specific IT Courts within Pakistan and the fact that electronic wills were not given legal force even after the enactment of the ETO 2002 (Rafiq, W., & Waqas, M. B. (2023).

LEGAL LANDSCAPE IN THE UNITED STATES:

In the United States, the Cyberspace is slightly different, despite there being concerns over surveillance by the CIA and FBI, the intelligence agencies there are far less actively involved in mass surveillance unless the need arises to compromise those rights in favour of national security. The country has, time and again imposed more contemporary regulations depending on how much the technology had evolved. As a product of continuing deliberations, the country now has a relatively robust cyber law infrastructure than other nations. This could be due to the fact that the US is a super power and most prone to cyber security attacks or it could be due to the fact that it's a developed state, or both.

In the U.S, cyber-security concerns are tackled at both, the federal level and state level through, sector-specific statutes and regulations. The main cyber-security regulations include the 1996 Health Insurance Portability and Accountability Act (HIPAA), the 1999 Gramm-Leach-Bliley Act, and the Federal Information Security Management Act (FISMA). While the HIPAA addresses concerns in the health sector, The FISMA maintains cyber-security standards for federal government agencies and their contractors. Some other statutes are specific to a single subject matter like the Veterans Affairs Information Security Enhancement Act (Ashwin. (2020), passed in 2006 and they focus closely on a single government agency, which, in this case is the Department of Veterans

Affairs (VA). Plus, since US is a country where states can legislate separately, each state has a distinct cyber security framework and legislations designed to protect the privacy while providing enough discretion to the authorities that it balances the security threats.

Some laws, however, have been subject to criticism for being too regulatory and invasive. For instance, Computer Fraud and Abuse Act (CFAA) enacted by Congress in 1986, which makes it a crime to access and subsequently share protected information. At the same time, there are legislations such as the Electronic Communications Privacy Act, 1986 allowing the U.S. government to access electronic communications such as emails, social media messages, and more with a subpoena (McCaul, M. (2018) which has been criticized for the discretion it provides, however, it is imperative to provide law enforcement and authorities with such discretion in order for them to be able to protect the citizens to the best of their abilities. That is, only if the information is used for protection of citizens and that alone.

Some critics argue that it is more plausible to have a uniformly defined national cyber security framework and that the existence of cyber regulations at multiple levels and sectors has impacted compliance to a certain degree. Thus, in 2018, US President Donald Trump signed into law the Cyber security and Infrastructure Security Agency Act of 2018. However it does not appear to be the solution to any issues faced by the US, other than making the job of lawyers slightly easier. Whilst it is true that due to the cyber ransom-ware and phishing attacks becoming more complex the US will eventually require for there to be more cyber security professionals, it is not believed the infrastructure is weak enough to warrant attention.

The US has always taken cyber security threats seriously. Prominent examples include but are not limited to the Meta case and the TikTok case. Prior to the number of cases initiated against Facebook, in 2018, it was disclosed that Facebook had handed over information of over 87 million users to Cambridge Analytica by the New York Times and the Observer (The Economist, 2018). Analytica being a company expected to use the data to inform political campaigns caused the US Congress to take the matter extremely seriously and called Zuckerberg to testify. It resulted in Facebook being held liable to pay $725 million to settle the privacy lawsuit and better enforcement of the privacy regulations by the authorities . Similarly in 2023 the FBI and the US Justice Department initiated an investigation of TikTok and its potential involvement with the CCP. As before, the case is being taken extremely seriously and TikTok is expected to be partially or completely banned across the country. The Federal legislation has stagnated however the state legislatures have not, example would be Montana where Montana passed SB 419, which was titled appropriately ‘An Act Banning TikTok in Montana’ (Rinehart, W. (2024).

Another similar example occurred in July 2020 when twitter accounts of prominent celebrities and former presidents including Barak Obama and Donald J. Trump were hacked, partly due to negligence on part of the twitter employees, in order to promote a Bit Coin scam. Twitter moved quickly and secured the compromised accounts and similar haste was seen from the law enforcement agencies who apprehended the suspects and traced it back (Radford, J. T. (2023).

LEGAL FRAMEWORK IN EUROPEAN UNION:

The European Council has been prudent in addressing the dangers of the Internet in member states. Recently, the Council developed a framework to sanction cyber criminals who have committed cyber-attacks from outside of EU member countries or used any of infrastructures from a country other than an EU country, or are crimes performed with the help of a person sitting outside an EU member country. In 2022, Six criminal and three entities were sanctioned for committing the cybercrimes (Akhtar, S).

More recently the Council has established a comprehensive framework to regulate electronic transactions to avoid fraud and misappropriation of funds. Moreover the Council has put serious effort in dealing with cyber-attacks at the regional level without requiring aid from other

nations or entities. Cyberlaws are regulating such a rapidly evolving space that they are the ones most prone to becoming obsolete and hence the legislation has to be attentive of the contemporary issues and adjust them accordingly, which is what EU member states have generally practiced.

EU CYBERSECURITY LAWS

The Cybersecurity Act (EU 881 / 2019)	This act harmonized the cybersecurity certification process for the whole of EU, as prior to its enactment numerous certifications were required by businesses and consumers, causing the process to be lengthy and needlessly complicated. The Act further empowered European Union Agency for Cybersecurity (ENISA) to improve cybersecurity by giving it a permanent mandate across the EU.
The network and information security directive (NIS 2 Directive)	The NIS 2 Directive went through a revision in 2022. The one prior/original one was the first step in establishing good cyber security rules and other steps such as establishing the necessary cyber crisis management structure (CyCLONe) and covering a larger share of the economy and society by including more sectors, which implies that more entities are obliged to take measures in order to increase their level of cybersecurity etc. The more recent revision expands the scope of the original and assigns new tasks to ENISA such as the publication of an annual report on the state of cybersecurity in the EU and the development and maintenance of a European vulnerability registry etc. (ENISA, 2024)
The European General Data Protection Regulation	Endorsed in 2018, it is the most crucial piece of legislation for the entities working within the EU. Its concern is related to data protection, safeguarding personal data including privacy, and creating convenience in regulation processes for international organizations. What differentiates this from other regulations is its emphasis on individual privacy, data protection and the broader control it provides to EU citizens over their

	data.

COMPARATIVE ANALYSIS WITH USA AND EU:

Pakistan's approach, shaped by its sociopolitical dynamics and regional security concerns, was to establish a cyber-crime prevention legislation through the Prevention of Electronic Crimes Act (PECA). However, the efforts are being hindered by digital literacy gaps and resource constraints. On top of the fact Pakistan has institutions that retain such levels of power where they can arbitrarily infringe any individual's right to privacy without any legal repercussions. Pakistan critically needs to augment digital literacy and infrastructure to bolster cyber-security measures effectively, similarly the powerful institutions must not infringe the right to privacy of the individuals residing within unless it is a matter concerning national security but that is easier said than done. A balance of reasoning must be undertaken strictly in the utilitarian sense where the right to privacy of an individual must only be infringed once it is ascertained that the potential benefit would outweigh the harm. The USA has the most advanced technological approaches in all fields, therefore, the approach to cyber-security is also distinguished by its amalgamation of multiple elements that strengthen a strong defense against cyber threats. The advanced technological equipment and information is the basis for the implementation of modern security measures and innovations in cyber-defense. It has imperfect but extremely robust institutions dedicated to combat cyber-security such as the Department of Homeland Security (DHS) and the National Security Agency (NSA). (Watto, O. M., Islam, M., Hussain, S. A., & Shahab, M. (2024). These institutions are operating effectively by formulating policies, coordinating national security, and providing guidance on best practices for safeguarding against cyber threats. It is believed that the cyber-security framework in the US is far more developed than that of Pakistan possibly be due to it being a more developed country or due to it being a global superpower and hence requiring comparatively more investment than usual in the sector. Perhaps a combination of both, regardless there appears to be a consistent effort from the legislative wing to create better and more pragmatic cyber security laws, an effort which isn't replicated in Pakistan similarly.

In a similar fashion, it can be clearly observed that in the legal Framework of EU there is a strong emphasis on the right to freedom of expression and the right to freedom of speech. They are more adept at analyzing the changing technical space and hence are able to evolve rapidly in order to keep the laws pertinent enough(Akhtar, S). Plus the better implementation and administration causes it to surpass the level of cybersecurity Pakistan is at. Pakistan's problem appears to be multi-faceted; a less consistent attempt is seen from the legislature towards cybersecurity and an even worse issue is the implementation, the unnecessarily long and un-popular procedures and the incompetence which plagues the Pakistani law enforcement agencies. The legislature's lack of regard for the cyberspace could possibly be due to Pakistan facing more prominent and destructive threats like climate change and a rampant inflation. Regardless, the issues still remain, will continue to persist and evolve eventually.

CONCLUSION:

As can be deduced from the aforementioned discussion, the cyber laws in the EU, US and other similar developed nations are far more developed than that of Pakistan, which is expected. What is not expected however is the level of surveillance present in the country, the broken redressal system offered by the FIA and the sheer lack of Public awareness pertaining to these matters. The US has far better implementation of cyber laws as is observed on numerous occasions including prominent examples such as the TikTok and Meta cases. The level of surveillance in the US, however, is believed to be high, which could be justified, being a global superpower and hence being more prone to spies and national security threats, as long as the discretion is exercised cautiously. A similar sentiment can be observed in the developed EU countries, security does overpower the right to privacy in certain cases

after deliberations. Hence, the same could be applied to Pakistan; caution must be exercised.

Nonetheless, as the authors of this article it is of course understandable that the authors would consider cybersecurity to be something Pakistan should prioritize, however as a rational individual, it is not plausible to suggest that cybersecurity is the primary threat Pakistan is facing currently. The threats Pakistan is facing are far diverse in nature, ranging from democracy and an overburdened judiciary to climate change and other similar threats. Cybersecurity is definitely one of the concerns, and something Pakistan should not turn a blind eye to, but not something a rational individual would consider to be the top priority as of now, considering the political and economic state of the country. The instant and initial efforts Pakistan must make is to gradually move towards cybersecurity by enacting better legislations and administer their implementation as perfectly as possible. Something which can be done gradually, though it must not be ignored completely.

RECOMMENDATIONS:

- Privacy of the individuals must be preserved. The regulations must hence be amended to take away the discretion from the authorities to regulate constantly and should only be permitted to regulate when security threats are involved and/or when court warrants have been issued.
- Extra-legal authorities must be brought within the purview of law. At least to a certain degree, considering Pakistan's political dilemma, it is understandable that they cannot be completely brought under strict purview of law, however certain specific discretions must still be revoked.
- A more galvanized effort must be seen from the government to make the FIA procedure more transparent, less complicated and far less time-consuming. There is an acute need of a systematic overhaul of how exactly the FIA complaint procedure works and how the agency operates. Public awareness must also be raised specifically regarding how the FIA operates and regarding how legal redress can be sought from the agency.
- Cybersecurity and Research should be subsidized especially in the government sector in order for the sector to gradually grow and eventually be on par with that of the more developed states.

REFERENCES:

Adil, K. (2023). Legal Framework for Policing Cyberspace in Pakistan: An Overview. Retrieved from https://rsilpak.org/2023/legal-framework-for-policing-cyberspace-in-pakistan-an-overview/#:~:text=Based%20on%20this%20constitutional%20edifice,of%20Electronic%20Crimes%20Act%2C%202016.

Akhtar, S. (Year of publication not provided). Assessing the Cybercrime Legislation in Pakistan: A comparative study of European Union and Pakistani Cybercrime Laws. SSRN-id4555751 (1).pdf

al-Taj, H., Polok, B., & Rana, A. A. (2023). Balancing Potential and Peril: The Ethical Implications of Artificial Intelligence on Human Rights. *Multicultural Education*, *9*(6).

Amnesty International. (2022, September 29). Myanmar: Facebook's Systems Promoted Violence Against Rohingya; Meta Owes Reparations. Retrieved March 8, 2024, from https://www.amnesty.org/: https://www.amnesty.org/en/latest/news/2022/09/myanmar-facebooks-systems-promoted-violence-against-rohingya-meta-owes-reparations-new-report/

Ashwin. (2020). Analysis of Cyber Laws in USA, UAE and Germany. Retrieved from https://enhelion.com/blogs/2020/11/24/analysis-of-cyber-laws-in-usa-uae-and-germany/#_ftn3

Bukhari, F. H. (2014). Pakistan Dominates The Surveillance Hall Of Shame. Retrieved from https://www.giswatch.org/: https://www.giswatch.org/en/country-report/communications-surveillance/pakistan#_ftn19

Constitution of Islamic Republic of Pakistan. (1973). Article 14. https://na.gov.pk/uploads/documents/1549886415_632.pdf

Fazi, H. F. S., Shaikh, M. A., & Rana, A. A. (2023). Jurisprudential Styles: Reasoning from Textual Expressions and Its Examples: A Research Review. *INKISHAF*, *3*(8), 439-460.

Iqbal, S. (2023). The legal landscape for privacy and surveillance in Pakistan. https://www.ibanet.org/legal-landscape-for-privacy-surveillance-in-Pakistan#:~:text=In%20Pakistan%20the%20right%20to,the%20constitutional%20right%20to%20life.

Jamshed, J., & W. R. (2022). Critical Analysis of Cybercrimes in Pakistan: Legislative Measures and Reforms. Retrieved from https://ijbea.com/: https://ijbea.com/ojs/index.php/ijbea/article/view/234/197

Khan, E. A. (Year of publication not provided). The Prevention of Electronic Crimes Act 2016: An Analysis. Retrieved from https://sahsol.lums.edu.pk/node/12862#:~:text=Freedom%20of%20Speech,the%20cornerstones%20of%20democratic%20institutions.

Majid, A., Haider, I., Babr, K., & Saad, M. (2018). Cyber Crime Laws in Pakistan. Retrieved from Cyber_Crime_Laws_in_Pakistan.pdf

McCaul, M. (2018). H.R.3359 – 115th Congress (2017-2018): Cybersecurity and Infrastructure Security Agency Act of 2018. Retrieved November 12, 2020, from https://www.congress.gov/bill/115th-congress/house-bill/3359

Monroe College. (2024). Cybersecurity History: Hacking & Data Breaches. Retrieved from https://www.monroecollege.edu: https://www.monroecollege.edu/news/cybersecurity-history-hacking-data breaches#:~:text=Technically%2C%20the%20very%20first%20cyberattack,that%20things%20got%20really%20interesting.

Pound, R. (1981). An introduction to the philosophy of law. Clarendon Press. https://lib.ui.ac.id/file?file=digital/20383519

Radford, J. T. (2023, May 10). Briton pleads guilty in US to 2020 Twitter hack. Retrieved from https://www.bbc.com/: https://www.bbc.com/news/technology-65540901

Rafiq, W., & Waqas, M. B. (2023). An Appraisal of Pakistan's Electronic Transaction Law and Certification Service Providers' Accreditation Regulations. Journal of Law & Social Studies (JLSS), 5(2), 307-321. Retrieved from https://www.advancelrf.org/wpcontent/uploads/2023/07/Vol-5-No.-2-15.pdf

Rana, A. A. (2020). Admissibility of Evidence Produced via Modern Devices and Techniques: A Look in Pakistani Prospective. *International Journal of Research*, *8*, 67-77.

Rana, A. A. (2021). Admissibility of Dying Declaration as Evidence: The Case of Pakistan. *IUP Law Review*, *11*(4).

Rana, A. A. (2021). Role of Corporate Finance Law in Corporations. *International Journal of Research*, *8*, 96-107.

Rana, A. A. (2022). The right of custody of minor: A comparative study of Sharī'ah and Pakistani legal system. *International Journal of Human Rights and Constitutional Studies*, *9*(4), 350-368.

Rana, A. A., & Siddique, H. M. (2022). The Transgender Persons (Protection of Rights) Act 2018: A Shariah appraisal of self-perceived gender identity and right of inheritance of the transgender. *Competitive Educational Research Journal (CERJ)*, *2*, 77-88.

Rana, A. A., & Zahid, R. Q. (2021). Competition law and digital technologies in Pakistan: critical analysis. *Al-KASHAF (Research*

Journal of Legal and Social Studies) July, *1*(2).

Rana, A. A., Ali, A., & Hussain, Z. (2022). Unification of Corporate Governance (CG) Model in the European Union and Brexit: An Analytical View. *Pakistan Journal of Social Research*, *4*(2), 626-634.

Rana, A. A., Gujjar, U. A., Ahmad, F. Z., & Naul, A. H. K. (2022). Admissibility and Evidentiary Value of Electronic Evidence in Criminal Cases: A Case Study of Pakistan. *JL & Soc. Pol'y*, 27.

Rana, A. A., Hussain, B., & Hussain, Z. (2022). Legal and Social Review of Child Marriage in Pakistan: A Judicial Perspective. *Available at SSRN 4145917*.

Rana, A. A., Tirmazi, S. M. S., Fatima, K., Din, M. A. U., Ahmad, I., & Zulfiqar, F. (2023). The Juridical Contribution of the Federal Sharīʿat Court (Fsc) In the Islamization of Laws in Pakistan: A Study of Leading Cases. *Al-Qanṭara*, *9*(4), 91-104.

Rana, A. A., Zulfiqar, F., & Masuad, S. (2023). The Legal and Regulatory Framework for Cryptocurrency and Fintech in Pakistan: Challenges and Policy Recommendations. *Available at SSRN 4426294*.

Razi, N., & Zahoor, R. (Year of publication not provided). Analyzing the Cyberspace Laws to Protect Data Privacy in Pakistan. Retrieved from file:///C:/Users/Ilma/Downloads/RDET_v13_n2_42to55%20(1).pdf

Rinehart, W. (2024, January 30). The Complex Case of TikTok in the United States. Retrieved March 3, 2024, from https://www.thecgo.org: https://www.thecgo.org/research/the-complex-case-of-tiktok-in-the-us/

Sheikh, M. A., Bin Ahmed, S. M., & Rana, A. A. (2023). Economic Security in Pakistan: Indicators, Issues, Impacts and Way Forward. *Issues, Impacts and Way Forward (June 30, 2023)*.

Supreme Court of Pakistan. (1998). Mohtarma Benazir Bhutto And Another v. President Of Pakistan And Others (P L D 1998 Supreme Court 388). Retrieved from https://www.digitalrightsmonitor.pk/wp-content/uploads/2021/01/Mohtarma-Benazir-Bhutto-vs-the-President-of-Pakistan.pdf

The Economist. (2018, April 9). Why is Mark Zuckerberg testifying in Congress? Retrieved March 8, 2024, from https://www.economist.com/: https://www.economist.com/the-economist-explains/2018/04/09/why-is-mark-zuckerberg-testifying-in-congress

Tribune.pk. (2023, July 07). Cyberattack on ECP; security alert issued. Retrieved from https://tribune.com.pk/: https://tribune.com.pk/story/2425168/cyberattack-on-ecp-security-alert-issued

United Nations General Assembly. (1948). Universal Declaration of Human Rights. https://www.un.org/en/about-us/universal-declaration-of-human-rights#:~:text=Drafted%20by%20representatives%20with%20different,all%20peoples%20and%20all%20nations.

United Nations General Assembly. (1989). Convention on the Rights of the Child. Retrieved from https://www.ohchr.org/en/professionalinterest/pages/crc.aspx

Watto, O. M., Islam, M., Hussain, S. A., & Shahab, M. (2024). Cyber Law and Cyber Security Policies in Pakistan: A Comparative Study with USA, Canada and Australia. Retrieved from https://journals.internationalrasd.org/index.php/pjhss/article/view/1977/1325