



YOUTH GENERAL ASSEMBLY

Gender

& Cybercrime in Pakistan

www.ygapakistan.org

Youth General Assembly (YGA) is an autonomous organization dedicated to providing a credible platform that fosters policy and strategy development, equitable administration, and non-traditional legislative activities. YGA empowers young individuals to engage in public discourse on social issues, preparing them to be future ambassadors and democratic leaders. Our mission is to inculcate the qualities of convening and engagement among the youth, expanding their perspective and knowledge of true democracy and parliamentary politics.

Copyright © Youth General Assembly (YGA)

All Rights Reserved

Printed in Pakistan

Any part of this publication can be used or cited with a clear reference to Youth General Assembly.



YOUTH GENERAL ASSEMBLY

Table of Contents

1) What is Cyber Crime? -----	3
2) 2 Cyber Crime Act in Pakistan -----	3
3) 3 PECA 2016 penalties for Cyber Criminals -----	3
4) 4 Statistical Data -----	3
5) 5 PECA 2016 Comparison with UK Data Protection Act 2018 -----	4
6) 6 Cyber Crime dealt under PECA 2016 -----	4
7) 7 Federal Investigation Agency and its role -----	4
8) 8 PECA 2016 enactment by the National Assembly -----	5
9) 9 Code of Criminal Procedure 1860 -----	6
10) 10 Pakistan Penal Code 1860 -----	7
11) 11 Amendment in PECA 2016 -----	7
12) 12 Citizens Protection (Against online Harm) 2020 -----	8
13) 13 Case study on Cyber Crime -----	8
14) 14 PECA 2016 preamble that the investigation is observed by FIA -----	9
15) 15 Conclusion -----	9

1. What is Cybercrime?

Cybercrime refers to criminal acts committed using computing devices and the internet. These offenses are typically carried out against individuals or groups with the intent to harm the victim's reputation or cause psychological distress. Cybercrime encompasses a range of activities, including hacking, cyberbullying, cyberstalking, spoofing, intellectual property theft, digital piracy, and more.

2. Cyber Crime Act in Pakistan

The law governing cybercrimes in Pakistan is the **Prevention of Electronic Crimes Act (PECA)**, introduced in 2016. It provides a comprehensive framework to address various types of cybercrime in the country. This act deals with several internet-related offenses, including:

- Illegal access to data
- Denial of service attacks
- Cyber terrorism
- Electronic forgery and fraud
- Spamming, which refers to unsolicited messages such as posts on the internet, emails, and text messages. Spamming has become increasingly prevalent on social media, where unwanted spam content frequently appears on social networking platforms.

3. PECA 2016 Penalties for Cyber Criminals

The **Prevention of Electronic Crimes Act (PECA) 2016** outlines penalties for cybercriminals in Pakistan, including:

- Up to 3 years of imprisonment, a fine of 1 million PKR, or both for unauthorized access to critical information systems.
- Up to 7 years of imprisonment, a fine of 10 million PKR, or both for disrupting critical information systems with dishonest intent. The same penalty applies to cyber terrorism cases.
- Up to 3 years of imprisonment, a fine of 5 million PKR, or both for involvement in data breaches, including the online distribution of someone's personal data without consent.

4. Statistics

Cyber-crime in Pakistan has increased by 83pc in three years, reports, The news on 28 August 2021. The data given shows that the cybercrimes complaints have shot up increasingly, up to 83pc from 2018 to 2020 ^[1]

In 2018, the cybercrime wing dealt with a total of 16,122 complaints and in 2020 the number was 94,000. Out of which over 44,000 complaints related to financial frauds were registered and dealt with in the span of the past 3 years. The other complaints were harassment, 15,000 hacking, 10,358 defamation and 16,601 complaints of fake profiles were registered from the year 2018 to 2020 ^[2]

1 Kasim Abbasi, 'Cybercrime increases by 83pc in three years' International THE NEWS <<https://www.thenews.com.pk>> (28 August 2021)

2 Ibid

5. PECA 2016 Comparison with UK Data Protection Act 2018

Similarly, the United Kingdom has a law comparable to Pakistan's **Prevention of Electronic Crimes Act 2016**, known as the **Data Protection Act 2018**. This law holds individuals and organizations responsible for handling personal data and requires them to follow strict guidelines, known as the 'data protection principles.' These principles ensure that personal data is used fairly, lawfully, and transparently.

The act also mandates that appropriate security measures are in place to protect against unlawful and unauthorized data processing. When comparing Pakistan's PECA with the UK's Data Protection Act, it is clear that the UK legislation provides more robust legal protections, particularly concerning sensitive issues like political opinions and ethnic backgrounds.

6. Cyber Crime dealt under PECA 2016

Cybercrime-related offenses are addressed under the **Prevention of Electronic Crimes Act 2016**, as mentioned earlier. These include **child pornography**, which is a form of child sexual exploitation involving any visual depiction of sexually explicit conduct that features a minor.

Additionally, **cyberstalking** has become increasingly common due to the rise in electronic communication being used to harass or threaten individuals.

These digital crimes are often linked to the **dark web**, a part of the internet that can only be accessed through special software, allowing users and web operators to remain anonymous. However, the dark web is often associated with illegal activities. In software license and service agreements, liability clauses often include detailed provisions regarding cybersecurity, hacking, data protection, and infringement of another party's copyrighted content. Frequently, data is stored on platforms like Google Drive, and if an account is hacked, liability can become unlimited.

7. Federal Investigation Agency and its role

These crimes are closely related to the **Prevention of Electronic Crimes Act 2016**. Investigations into such crimes are conducted by various investigative agencies, and in Pakistan, they are overseen by the **Federal Investigation Agency (FIA)**. However, in a recent update, the Islamabad High Court declared PECA 2016 unconstitutional. The court ruled that the offense under **Section 20** of the Act contradicts the Constitution, as its broad phrasing not only covers defamation but also allows for the arrest and imprisonment of individuals. This, in turn, creates a chilling effect on free speech, which violates constitutional protections. The court's decision to invalidate Section 20 was made beyond a reasonable doubt.

The Cybercrime Wing of the FIA operates under the guidance of PECA 2016 and is responsible for addressing the growing threats of cybercrimes in Pakistan. It is the only unit in the country that directly handles complaints and takes legal action against cybercriminals, aiming to curb technological abuse in society.

In May 2022, the FIA issued a warning to overseas Pakistanis allegedly involved in committing offenses on social media, stating that their names could be placed on the Exit Control List (ECL) and that Interpol red notices could be issued for their arrest^[3].

The FIA has been working diligently to combat cybercrime in Pakistan. Recently, the FIA initiated action against Sadaqat Hussain, who was running fake Twitter accounts impersonating retired army officers. During interrogation, the accused admitted to using social media to distribute fake video clips of various retired Generals. An investigation is currently underway to uncover the motive behind his actions^[4].

Recently, the FIA arrested an individual for creating a fake Twitter account impersonating Prime Minister Shahbaz Sharif. The person was using social media to falsely represent the Prime Minister. A case has been registered against the accused, and legal proceedings are underway^[5].

Currently, every cybercrime complaint is categorized into subsections. The FIA first verifies each complaint and initiates an inquiry once it passes the verification process. If an offense is identified, the inquiries are further translated into criminal cases. The FIA has made it easier to register cybercrime complaints by providing a cybercrime complaint registration form on their website. Once the details of the crime and its category are filled in, the form can be submitted online.

According to statistics published in a Dawn article in January 2022, a total of 102,356 complaints were made the previous year. Of these, 80,641 went through the verification process, with 15,932 moving to the inquiry stage. Ultimately, 1,202 cases were registered under PECA 2016, and over 1,300 suspects were arrested^[6].

The FIA works in coordination with Interpol by issuing red notices through a specific process. The FIA contacts Interpol through the District Police Officer or the officer in charge from the requesting law enforcement agency. The request for issuing an Interpol notice is forwarded to the Inspector General of Police, who then submits it to the home department of the Provincial Government. From there, it is sent to the Ministry of Interior in Islamabad for approval. After approval, the Ministry of Interior refers the request to the Director-General of FIA, who leads NCB-Interpol in Islamabad.

For instance, in cases of child pornography, the FIA was able to apprehend suspects based on information provided by Interpol.

8. PECA 2016 Enactment by the National Assembly

In 2016, the National Assembly enacted the Prevention of Electronic Crimes Act (PECA) to provide a comprehensive legal framework for defining various types of electronic crimes, as well as establishing mechanisms for the investigation, prosecution, and adjudication of these crimes.

3Noor Aftab, 'FIA warns overseas Pakistanis' <https://www.thenews.com.pk> (9 May 2022)

4 Pakistan, Man Behind fake Twitter accounts of ex- Army officers detained <https://dailytimes.com.pk> (25 May 2022)

5 FIA arrests man for impersonating PM Shehbaz Sharif on Twitter <https://arynews.tv> (23 May 2022)

6 Azfar-ul-Ashfaq, 'Cybercrime complaints topped 100,000 in 2021: FIA Chief' Dawn <<https://dawn.com>> (Karachi, Pakistan, 3 January 2022)

According to Section 2(1)(a) of the Act:

- **S.2(1)(a)(i)** refers to a series of acts or omissions that are contrary to the provisions of this Act.
- **S.2(1)(a)(ii)** covers causing an act to be done by a person either directly or through an automated information system, automated mechanism, or a self-executing, adaptive, or autonomous device, whether the impact is temporary or permanent ^[7].

This means that any act committed as a cybercrime will be charged under the Prevention of Electronic Crimes Act 2016 (PECA). The authority referenced in this Act is the Pakistan Telecommunication Authority (PTA), which was established under the Pakistan Telecommunication (Re-organization) Act 1996 (Act XVII of 1996). It also implies that authorization under this law must be granted either by law itself or by a person legally empowered to issue such authorization ^[8].

The offenses and punishments under the Prevention of Electronic Crimes Act (PECA) 2016 include unauthorized access to an information system or data. This means that whoever, with dishonest intent, gains unauthorized access to any information system will face imprisonment of up to 3 months, which may be extended. Interference with an information system or data can result in imprisonment of up to 6 months, an extension of that term, or a fine that may go up to one hundred thousand rupees, or both.

Moreover, glorification of an offense refers to any act where an individual prepares or disseminates information through any information system or device with the intent to glorify an offense related to terrorism. This includes cyberterrorism, which causes fear, insecurity, and panic among the public and government. Additionally, it can incite interfaith, ethnic, or racial hatred, leading to hate speech. Such offenses are punishable by a term of up to 14 years or a fine that may extend to 50 million rupees.

The establishment of investigation agencies and the delegation of procedural powers for investigations under PECA 2016 allow the federal government to establish or delegate law enforcement agencies for the purpose of investigation. Authorized officers of these agencies have the power to investigate. A warrant for a search may be issued by the court based on the satisfaction of an authorized officer who demonstrates that reasonable grounds exist for a specified criminal investigation or proceedings.

International cooperation can be provided upon the request of the federal government. Such cooperation can be extended to any foreign government, foreign agency, or international organization through a designated agency under this Act for the purposes of investigations or proceedings related to offenses involving information systems.

9. Code of Criminal Procedure 1860

Prosecution and trial of offenses are categorized as compoundable, cognizable, and non-cognizable under Section 4(1)(f) and Section 4(1)(n) of the Criminal Procedure Code 1860. **A**

⁷ Prevention of Crimes Act 2016, S.2(1)(a) https://na.gov.pk/uploads/documents/1472635250_246.pdf

⁸ Ibid

cognizable offense is defined as one where a cognizable case exists, meaning that a police officer is authorized, under the second schedule or any applicable law, to arrest the offender without a warrant ^[9].

A non-cognizable offense refers to an offense, and a non-cognizable case means a case in which a police officer cannot arrest without a warrant. Offenses that fall under abetment are non-bailable. On the other hand, the prosecution and trial of cognizable offenses are handled by presiding officers of the court, designated by the federal government in consultation with the Chief Justice of the respective High Courts, at locations deemed necessary. In the case of cognizable offenses, investigative agencies may proceed without prior court permission. However, for non-cognizable offenses, court permission is required before an investigation can begin. For example, Sections 17, 19, and 21 of the PECA 2016 fall under this category.

To prevent electronic crimes, the federal government or the authorized authority can issue directives to be followed by designated information systems and service providers. The creation of Computer Emergency Response Teams is also mandated, tasked with recording incidents and responding to any threats or attacks on critical information systems in Pakistan. These teams are to be established by the federal government.

10. Pakistan Penal Code 1860

This act in relation to the other laws of Pakistan, as the provision of this act, has no derogation of the Pakistan Penal Code 1860, as a matter of fact The PECA 2016 and PPC work better together, such as Section 354 of the PPC which deals with modesty, harassment etc. The further act includes the Code of Criminal Procedure 1898, The Qanoon-e-Shahadat order 1984, The Protection of Pakistan Act 2014, and the investigation of for The Fair trial Act 2013^[10].

The Pakistan Penal code 1860 was amended and the code of Criminal Procedure, 1898, added more sections. In which Section 292B was added which is related to child Pornography, whoever takes, permits to be taken, with or without the consent of the child or with or without the consent of his parents or guardian, any photograph, film, video, picture or representation, portrait, or computer generated image or picture, whether made or produced by electronic, mechanical, or other means, of obscene or sexually explicit conduct, where there is a visual depiction that involves a minor a boy or girl engaging in obscene or sexually explicit conduct^[11].

The Pakistan Penal Code 1860, Section 500 deals with punishment for defamation, whoever defames another shall be punished with simple imprisonment for a term which may extend to two years, or with a fine, with both ^[12].

9 Criminal Procedure Code 1860, S.4(1)(f) & S.4(1)(n)

10 Prevention of Crimes Act 2016, S.2(1)(a) https://na.gov.pk/uploads/documents/1472635250_246.pdf

11 The Pakistan Penal code, 1860 and the Code of Criminal Procedure, 1898, Section 292B
https://senate.gov.pk/uploads/documents/1450099224_165.pdf

12 Pakistan Penal Code (ACT XLV OF 1860), Section 500
<https://www.ma-law.org.pk/pdf/PAKISTAN%20PENAL%20CODE.pdf>

11. Amendment in PECA 2016

The **Prevention of Electronic Crimes Act (PECA) 2016** was introduced amidst growing concerns about the need to regulate cybercrimes. A recent amendment to the Act has introduced several changes, including making "online defamation" a non-bailable offense. This means that bail in online defamation cases will now be granted as an exception rather than a right, and the arrest of an alleged offender can be made without a warrant.

PECA 2016 works in conjunction with **Section 497 of the Criminal Procedure Code (CrPC) 1898** ^[13], which generally allows bail for offenses where the sentence is less than 10 years and does not fall within the scope of prohibitory clauses. These offenses are typically bailable, as established in **PLD 1995 SC 34**, which outlines the conditions under which bail may be granted:

1. The person cannot tamper with prosecution evidence.
2. The person is not an absconder.
3. The person has no previous criminal convictions or negative character history.
4. The person does not pose a danger to society and is not creating violence ^[14].

Understanding this process is important because in many **PECA 2016** cases, these sections are often set aside when applying **Section 497** of the CrPC, which deals with the prohibitory clause. Accused individuals often obtain bail under this section, demonstrating the limited power of PECA.

The Supreme Court has shown progressive trends in interpreting such cases. In **SCMR 526 (2022)**, the Supreme Court dealt with a case of cyberstalking and the transmission of objectionable images of a woman. The accused applied for bail, arguing that the offenses did not fall within the prohibitory clauses of **Section 497 of the CrPC**. The Court held that, typically, in cases falling outside the remit of the "prohibitory clause," bail is granted after the investigation is concluded. However, the Court noted that this practice is not without limitations. In the case at hand, the privacy of a young woman had been gravely violated, causing embarrassment to her family and jeopardizing her marriage. The incident was reported by her father-in-law, and in light of the facts, the concurrent view of the lower courts in denying bail was correct. The petition for leave to appeal was dismissed, and the accused was refused bail ^[15].

The recent amendment to PECA has also increased the maximum sentence for offenses from 3 years to 5 years. These changes suggest that the regime seeks to closely monitor and control dissenting voices and discourse. One major drawback of PECA is that most offenses under **Sections 10, 21, and 22** are non-cognizable offenses, meaning no FIR will be lodged, and investigative agencies like the FIA or police cannot begin investigations without a magistrate's permission ^[16].

13 The Code of Criminal Procedure, 1898, Section 497

14 PLD 1995 SC 34

15 2022 SCMR 526

16 By admin, "The PECA Amendment: Reputation or right to speak?" <<https://rcilhr.com>> accessed on 26 March 2022

12. Citizen’s Protection (Against online Haram) 2020

In January 2020, the federal Cabinet of Pakistan approved the Citizen’s Protection (Against online Harm) rules to regulate social media platforms for streaming content related to terrorism, extremism, hate speech, sedition, fake news, violence, defamation and national security ^[17]

13. Gender Perspective on Cybercrime:

Why are women not welcome on the internet?

Countries like the USA and the United Kingdom have long supported gender mainstreaming to promote gender equality in their legal systems. Similarly, Pakistan is making efforts in this area. Article 25 of the Pakistani Constitution ensures equality before the law, while Articles 25(3) and 26(2) allow the state to make special provisions for the protection of women and children. These provisions aim to provide extra protection, but despite these safeguards, some women and girls remain more vulnerable to cyberstalking and harassment than others. Over the past few years, cyber misogyny has been on the rise, reflecting the patriarchal and misogynistic trends from the offline world.

On World Press Freedom Day, UN Special Rapporteur Irene Khan emphasized the need for states to protect women journalists from both online and offline attacks. She also urged social media companies to ensure that online spaces are free from discrimination and safe for all women. While the internet serves as a powerful tool for democratization, it has also become a platform for perpetrators to spread hate speech and harass men and women alike—though women are disproportionately targeted.

A report by the Digital Rights Foundation (DRF) highlighted that WhatsApp and Facebook are the most common platforms where Pakistani women experience harassment. Women are statistically more likely to be harassed than men, and the social taboo surrounding female harassment is a key reason why many cases go unreported, leaving many women as silent survivors of abuse. A lack of exposure to the internet and digital awareness also leaves some women unequipped to respond effectively to online threats.

Public figures often become targets of cyber harassment. For instance, Pakistani actress Ayesha Omar faced severe cyberbullying and was frequently criticized for her clothing choices. Similarly, American actress Blake Lively has been subjected to body-shaming comments online throughout her career. A survey by Pew Research Center in the USA found that young women are more likely to experience online sexual harassment than men. Thirty-three percent of women under the age of 35 reported experiencing sexual harassment online, and 61% of American women view online harassment as a significant problem.

The Digital Rights Foundation in Pakistan has launched a helpline to assist victims of cyberstalking, spoofing, and bullying, offering support for a safer digital environment. Advocacy for the right to privacy, which is guaranteed under Article 14(1) of the Pakistani Constitution, is a critical part of these efforts to protect women online.

17 Citizen’s Protection (Against online Harm) Rules 2020

14. Case Study on Cybercrime

Pakistan Broadcasters Association v. Pakistan Electronic Media Regulatory Authority

The appellants in this case challenged the vires (legal authority) of Rule 15(3) of the Pakistan Electronic Media Regulatory Authority (PEMRA) Rules, 2009, and Clause 10.4 of the licenses granted to appellants Nos. 2, 4, 6, 8, and 10. They filed a petition before the Sindh High Court, contesting the legality of the notices issued under the rule. However, their petition was dismissed by a learned Division Bench of the High Court.

The appellants, who own and operate various satellite TV channels under licenses issued by respondent No. 1 (PEMRA), argued that they were compelled to accept the inclusion of Clause 10.4 in their licenses. This clause imposed a restriction on the maximum duration of advertisement breaks during prime time. The appellants contended that this restriction was unlawful, unreasonable, arbitrary, excessive, and disproportionate. They further argued that it amounted to an infringement on their managerial powers to determine what content, and when, should be broadcast by independent TV channels.

The appellants asserted that the restriction imposed by PEMRA went beyond the regulatory powers granted to the authority under Article 19 of the Constitution of Pakistan, 1973, which protects freedom of speech and expression, including freedom of the press ^[18].

The **Supreme Court of Pakistan** held that freedom of speech is fundamental to the natural rights of a civilized society. The state has a legitimate interest in regulating this right, especially when it conflicts with the rights of other individuals or broader societal interests. The Court emphasized that restrictions and duties must coexist to protect and preserve the right to free speech.

There is no doubt that freedom of speech is central to a society's right to impart and receive information on matters of common interest. It aids individuals in self-fulfillment, facilitates the discovery of truth, enhances the ability of individuals to participate in decision-making, and provides a mechanism to achieve a balance between stability and social change.

PECA 2016 Preamble that the Investigation observed by FIA

As the PECA 2016 preamble, has a special law for prevention and investigation of the prosecution and the trial of cybercrimes. It has been observed that the FIA, an investigation agency under the section 29 of the PECA invokes the provision of the FIA Act, 1974 in conducting the inquiries related to the offences defined under the PECA which may not be correct ^[19].

18 2016 PLD 692

19 Nasir Ayyaz, 'Reviewing Peca's powers' <https://www.dawn.com> accessed on 28 March 2022

The advent of the digital age has created a need for a robust cybercrime legislation that needs to be formulated by the nation states. As my countries around the world are struggling with drafting comprehensive laws in this regard. As the technological developments have outpaced the solutions that are proposed by the state institutions, which helps in addressing new challenges which are arising from the increased use of the digital media.

Conclusion

In conclusion, combating cybercrime requires a comprehensive approach that involves coordinated efforts from the government, law enforcement, legal professionals, and society as a whole. While laws like the **Prevention of Electronic Crimes Act 2016** have made significant strides in addressing unauthorized access to information, there is still much work to be done. Governments must continue to strengthen cybersecurity regulations and establish rapid response units to handle cyber threats effectively.

Law enforcement agencies need to be well-equipped to investigate cybercriminals, while legal professionals should focus on defending victims' rights. The judiciary has a crucial role in ensuring justice for those affected by these crimes. At the same time, individuals must take personal responsibility for securing their online presence by regularly updating privacy settings and remaining vigilant against potential threats. Ultimately, it is only through a collaborative effort that society can effectively combat cybercrime and create a safer digital environment for everyone.

Bibliography

Legislation

1. Data Protection Act, 2018
2. S.2(1)(a) Prevention of Crime Act 2016
3. S.4(1)(f) & S.4(1)(n) The Pakistan Penal code,1860 & Criminal Procedure Code 1898
4. Section 292B Criminal Procedure Code 1860
5. Section 500 Pakistan Penal Code (ACT XLV OF 1860)
6. Section 497 The Code of Criminal Procedure, 1898
7. Citizen's Protection (Against online Harm) Rules 2020

Case Laws

1. PLD 1995 SC 34
2. 2022 SCMR 526
3. 2016 PLD 692

References

1. Azfar-ul-Ashfaque, 'Cybercrime complaints topped 100,000 in 2021: FIA Chief' Dawn <<https://dawn.com>>
2. By admin, 'The PECA Amendment: Reputation or right to speak?' <<https://rcilhr.com>>
3. FIA arrests man for impersonating PM Shehbaz Sharif on Twitter <https://arynews.tv>
4. Kasim Abbasi, 'Cybercrime increases by 83pc in three years' International THE NEWS <<https://www.thenews.com.pk>>
5. Nasir Ayyaz, 'Reviewing Peca's powers' <https://www.dawn.com>
6. Noor Aftab, 'FIA warns overseas Pakistanis' <https://www.thenews.com.pk>
7. Pakistan, Man Behind fake Twitter accounts of ex- Army officers detained <https://dailytimes.com.pk>
8. Tahir Naseer, 'IHC strikes down Peca ordinance, terms it 'unconstitutional'' <https://www.dawn.com>
9. <https://www.pewresearch.org/internet/2021/01/13/the-state-of-online-harassment/>
10. <https://digitalrightsfoundation.pk/>



Statutory Review By:
Aamna Hashmi & Maryam Zahid

      | [ygapakistan](https://www.youtube.com/ygapakistan)