Digital Democracy Initiative | PEACE AND JUSTICE NETWORK پیس اینڈ جسٹس نیٹ ورک پاکستان | CIVICUS

PECA
PREVENTION OF ELECTRONIC CRIMES ACT

Know the PECA: Do's and Don'ts for HRDs by PJN Pakistan

The Prevention of Electronic Crimes Act (PECA) 2016, along with its 2025 amendments, is Pakistan's main law regulating online activities. It covers areas such as online harassment, cyberstalking, fake or false information, hacking, and the misuse of social media. While PECA is designed to protect citizens and public order, its broad and sometimes vague provisions can put human rights defenders (HRDs) including journalists, lawyers, activists, and NGO staff at risk if they are not aware of their rights and obligations.

This guidance is designed to help HRDs work safely in the digital space, understand the law, and avoid unintentional legal exposure while continuing their essential work of defending human rights, reporting abuses, and promoting civic participation.

What This Document Does

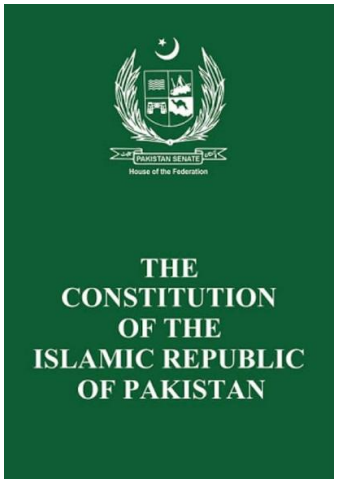
- **Simplifies the Law:** Breaks down PECA sections into plain language and explains how they affect daily digital work.
- **Provides Practical Guidance:** Offers actionable Do's & Don'ts to protect personal and professional digital security.
- **Supports Legal Preparedness:** Shows how to document, report, and respond to threats safely.
- **Promotes Safe Civic Space:** Ensures that HRDs can continue working online while safeguarding vulnerable communities and maintaining public trust.

Freedom of Expression Protected under Constitution and International Covenant

ICCPR (International Covenant on Civil and Political Rights)

- Article 19: Freedom of opinion and expression (including the right to seek, receive, and impart information and ideas of all kinds).
- Article 20: Prohibitions on advocacy of national, racial, or religious hatred constituting incitement to discrimination, hostility, or violence (sets legitimate limits).
- Article 21–22: Peaceful assembly and association (often implicated in expression-related cases).
- Article 14: Fair trial rights relevant to journalists/activists facing prosecutions for expression.

Constitution of the Islamic Republic of Pakistan (1973)



- Article 19: Freedom of speech, etc. (subject to reasonable restrictions in the interests of Islam, security, defense, public order, decency or morality, contempt of court, or incitement to an offense).
- Article 19A: Right to information (citizens' right to access information held by public bodies).
- Article 16: Freedom of assembly (supports expression through collective action).
- Article 17: Freedom of association (protects civil society and media unions).
- Article 10A: Right to fair trial (relevant when expression is criminalized).
- Article 14: Inviolability of dignity of man and privacy of home (often cited in balancing tests).

Legal Landscape — Laws HRDs Should Know

A. Prevention of Electronic Crimes Act (PECA)

Key sections often used:

Section 11 – Hate speech (linked with other laws)

Section 20 – Offences against dignity of a person

Section 21 – Cyber stalking

Section 24 – Hate speech

Section 37 – Power to remove or block content

Penalties may include fines and imprisonment.

B. Pakistan Penal Code (PPC)

Relevant sections:

- 499 & 500 – Defamation
- 503 – Criminal intimidation
- 505 – Statements creating public mischief

C. Punjab Defamation Act

Allows civil suits for online defamation.

How Authorities May Use These Laws

Laws can sometimes be applied broadly.

Examples:

- A tweet criticizing an institution may be labeled "false information."
- A report exposing corruption may be called "defamation."
- A repost may be treated as endorsement of alleged illegal content.

Even if a case is weak, the process itself can be stressful.This is why preventive caution and early legal support are critical.

Key Message

Understanding PECA and following these Do's & Don'ts empowers HRDs to continue defending rights, reporting abuses, and advocating for change, while minimizing legal risk and strengthening Pakistan's digital civic space.

1. Defamation & Harmful Content

Why it matters: Making false allegations about individuals or institutions can be treated as a criminal offence under PECA.

Relevant Sections

- **Section 20 (PECA 2025)** — Offences against dignity of a natural person

(1) Whoever intentionally and publicly exhibits or displays or transmits any information through any information system, which he knows to be false, and intimidates or harms the reputation or privacy of a natural person, shall be punished with imprisonment for a term which may extend to three years or with fine which may extend to one million rupees or with both.

☑ DO

- Base criticism on verified facts and evidence.
- Use careful language: *"According to verified reports…", "Allegations suggest…"*
- Keep records of sources and verification trail.

✗ DON'T

- Publish unverified allegations or accusations against any person.
- Share rumors, memes, or unconfirmed claims about crimes.
- Post sensitive details (names, associations) intended to injure reputation.

2. False Information & Misinformation

Why it matters: Publishing or spreading false or misleading content can attract imprisonment and heavy fines.

Relevant Sections

- **Section 26A (PECA Amendment 2025)** — Publishing information known or believed to be false that could cause fear or unrest.

26A, Punishment for false and fake information.—Whoever intentionally disseminates, publicly exhibits, or transmits any information through any information system,, that he knows or has reason to believe to be false or fake and likely to cause or create a sense of fear, panic or disorder or unrest in general public or society shall be punished with imprisonment which may extend upto three years or with fine which may extend to two million rupees or with both.

◇ Section 2 – New Definitions: The Amendment Act updates the definitions in the original PECA 2016, introducing new terms such as "aspersion" (spreading false and harmful information which damages reputation) and expanding what constitutes "unlawful" or "offensive" content in the digital context. These broadened terms are used throughout the law to justify content takedowns and penalties.

◇ Section 2R – Content Deemed False or False Information: This section deals with false or fake online content and empowered authorities to treat such content as unlawful, allowing them to block, remove, or penalise it even without detailed judicial oversight. The broad language of this section has been challenged as vague or open to misuse.

☑ DO	✗ DON'T
• Fact-check content before sharing. • Cross-verify using at least two credible sources. • Label provisional reports clearly when facts are still emerging.	• Post content that you know is false or have reason to believe is fake. • Amplify rumors, unconfirmed details, or speculative claims. • Ignore established journalism verification standards.

3. Cyber Harassment & Stalking

Why it matters: Targeting individuals with threatening or abusive behaviour online can lead to criminal charges.

Relevant Sections

- **Section 24(A) (PECA 2025)** Cyberbullying harassment and intimate image distribution.

24(A) Cyberbullying: (1) A person commits the offence of cyberbullying who, with intent to harass, threaten or target another person posts or sends electronic messages, including pictures or videos by using any social media platform, including chat rooms, blogs or instant messaging.

- **Section 24 (PECA 2025)** — Cyberstalking / persistent online threats.

24. Cyber stalking.— (1) A person commits the offence of cyber stalking who, with the intent to coerce or intimidate or harass any person, uses information system, information system network, the Internet, website, electronic mail or any other similar means of communication to—

(a) follow a person or contacts or attempts to contact such person to foster personal interaction repeatedly despite a clear indication of disinterest by such person;

(b) monitor the use by a person of the internet, electronic mail, text message or any other form of electronic communication;

(c) watch or spy upon a person in a manner that results in fear of violence or serious alarm or distress, in the mind of such person; or

(d) take a photograph or make a video of any person and displays or distributes it without his consent in a manner that harms a person.

(2) Whoever commits the offence specified in subsection (1) shall be punished with imprisonment for a term which may extend to three years or with fine which may extend to one million rupees or with both:

☑ DO	✗ DON'T
• Interact professionally and respectfully online. • Use clear, non-threatening language in public discussions. • Report harassment to platform authorities and legal support when needed.	• Engage in revengeful messaging, threats, or doxxing. • Persistently monitor or target critics or private individuals. • Post others' private media without consent.

4. Unauthorized Access & Data Security

Why it matters: Accessing or sharing others' digital accounts, systems, or information without permission is an offence.

Relevant Sections

- **Chapter II Offences and Punishments Section 3)** Unauthorized access to information system or data: imprisonment for a term which may extend to three months or with fine which may extend to fifty thousand rupees or with both.

☑ DO	✗ DON'T
• Seek consent before accessing or using someone else's digital account/data. • Employ secure and ethical data collection tools. • Use encryption and secure storage for sensitive evidence.	• Access emails, devices, cloud accounts, or systems without explicit trust/permission. • Download or publish leaked or pirated data.

5. Content Against Public Order, Security, Morality

Why it matters: PECA's definitions of "unlawful online content" may include content against public order, national security, or morality.

Relevant Sections

- **Section 37 (PECA 2025)** — Removal/blocking of "unlawful online content" including that against public order or national security.

37. Unlawful online content.— (1) 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 if it considers it necessary in the interest of the glory of Islam or the integrity, security or defence of Pakistan or any part thereof, public order, decency or morality, or in relation to contempt of court or commission of or incitement to an offence under this Act.

☑ DO	✗ DON'T
• Frame content in human rights and legal standards. • Focus on constructive critique rather than inflammatory language.	• Use words that could be read as incitement to violence, hatred, or upheaval. • Produce material that intentionally provokes disruption of public order.

6. Glorification of an offence, Cyber terrorism and Hate speech

Why it matters: Considered offences against State. In recent case, 17 year imprisonment given to human rights lawyers under Section 9 and Section 10 on post on Twitter and Reposting of that.

Relevant Sections

- **Section 9, Glorification of Offence, Section 10 Cyber Terrorism and Section 11 Hate Speech**

Section 9. Glorification of an offence.— (1) Whoever prepares or disseminates information, through any information system or device, with the intent to glorify an offence relating to terrorism, or any person convicted of a crime relating to terrorism, or activities of proscribed organizations or individuals or groups shall be punished with imprisonment for a term which may extend to seven years or with fine which may extend to ten million rupees or with both.

Explanation.—For the purposes of this section "glorification" includes depiction of any form of praise or celebration in a desirable manner.

10. Cyber terrorism.— Whoever commits or threatens to commit any of the offences under sections 6, 7, 8 or 9, where the commission or threat is with the intent to,— (a) coerce, intimidate, create a sense of fear, panic or insecurity in the Government or the public or a section of the public or community or sect or create a sense of fear or insecurity in society; or (b) advance interfaith, sectarian or ethnic hatred; or (c) advance the objectives of organizations or individuals or groups proscribed under the law, shall be punished with imprisonment of either description for a term which may extend to fourteen years or with fine which may extend to fifty million rupees or with both.

11. Hate speech.— Whoever prepares or disseminates information, through any information system or device, that advances or is likely to advance interfaith, sectarian or racial hatred, shall be punished with imprisonment for a term which may extend to seven years or with fine or with both.

☑ DO

- Verify Content Before Sharing
- Use Responsible Communication Channels
- Take Legal Opinion Before Sharing Sensitive Content

✖ DON'T

- Post content that praises or celebrates proscribed individuals/groups or content intended to intimidate
- Brand institutions with unfounded allegations.
- Use unverified narratives about judiciary or security forces.

7. Cyber Spam & Bulk Messaging

Why it matters: Unwarranted mass messaging, bulk emails or auto-messages can be penalized.

Relevant Sections

- **Section 25 (PECA 2025)** — Regulates "spamming".

25. Spamming.— (1) A person commits the offence of spamming, who with intent transmits harmful, fraudulent, misleading, illegal or unsolicited information to any person without permission of the recipient or who causes any information system to show any such information for wrongful gain.

(3) Whoever commits the offence of spamming as described in subsection (1) by transmitting harmful, fraudulent, misleading or illegal information, shall be punished with imprisonment for a term which may extend to three months or with fine of rupees fifty thousand which may extend upto rupees five million or with both.

☑ DO	✗ DON'T
• Use opt-in lists for newsletters or alerts. • Respect unsubscribe requests.	• Send unsolicited bulk messages to random numbers or emails.

8. Powers of an NCCIA Authorized Officer under PECA

Why it matters: Awareness of Authority Powers, Protecting Digital Privacy Responsibly and Compliance to Avoid Legal Risk.

Relevant Sections

- **Section 35. Powers of an authorized officer**

Section 35. Powers of an authorized officer.— (1) Subject to provisions of this Act, an authorized officer shall have the powers to—

(a) have access to and inspect the operation of any specified information system;
(b) use or cause to be used any specified information system to search any specified data contained in or available to such system;
(c) obtain and copy only relevant data, use equipment to make copies and obtain an intelligible output from an information system;
(d) have access to or demand any information in readable and comprehensible format or plain version;

(e) require any person by whom or on whose behalf, the authorized officer has reasonable cause to believe, any information system has been used to grant access to any data within an information system within the control of such person;
(f) require any person having charge of or otherwise concerned with the operation of any information system to provide him reasonable technical and other assistance as the authorized officer may require for investigation of an offence under this Act; and
(g) require any person who is in possession of decryption information of an information system, device or data under investigation to grant him access to such data, device or information system in unencrypted or decrypted intelligible format for the purpose of investigating any such offence:

☑ DO	✖ DON'T
• Keep Digital Data Organized and Documented • Implement Security Measures and data backups • Cooperate Legally with Authorized Officers	• Destroy or Hide Evidence • Share Unauthorized Data • Resist Arbitrarily

9. Harassment via Identity Misuse

Why it matters: Impersonating others online to cause harm or confusion is prohibited.

Relevant Section

- **PECA penalties related to impersonation/harm (context under 2016 framework).**
- **11. Hate speech.**— Whoever prepares or disseminates information, through any information system or device, that advances or is likely to advance interfaith, sectarian or racial hatred, shall be punished with imprisonment for a term which may extend to seven years or with fine or with both.

☑ DO	✖ DON'T
• Use your own verified accounts for official communication. • Keep consistent identity markers.	• Create fake profiles of others for mischief or advocacy

10. Reporting, Documentation & Legal Preparedness

Why it matters: If HRDs face PECA complaints or FIRs, documented evidence of good faith, verification, and compliance is critical.

Relevant Practice

- Not a single section but relevant to all offences for defence.

☑ DO	✖ DON'T
• Keep screenshots of posts with timestamps. • Maintain logs of editorial or verification processes. • Store source references and communication trails.	• Delete content or evidence after posting without backing it up — losing records weakens legal defence.

Quick Reminders for HRDs

- ◇ PECA's definitions are broad and can be interpreted expansively by law enforcement or courts, so caution and documentation are essential.
- ◇ Some parts of PECA (e.g., *old Defamation Section 20*) have been subject to constitutional challenge and judicial review, but that risk remains for online criticism.
- ◇ The 2025 amendments expand categories like "false information," "aspersions," and regulatory power, increasing the stakes for online content.

Final Tip

Use rights-based framing, verify everything you publish, and document your verification process. When in doubt, seek legal advice before sharing sensitive or controversial content online.

FIRST 24 HOURS INCIDENT RESPONSE CHECKLIST

for Human Rights Defenders

1 Log the Incident

Record the details of the incident immediately.

- ✓ What: Describe the incident (harassment, hacking, etc.)
- ✓ When: Date and time of occurrence

2 Secure Accounts & Devices

Immediately update passwords and secure devices.

- ✓ Change passwords for affected accounts and devices
- ✓ Enable two-factor authentication (2FA)
- ✓ Run antivirus and malware scans

3 Preserve Evidence

Document the incident and preserve evidence.

- ✓ Take screenshots of threatening message, profiles etc.
- ✓ Backup important data and evidence to a secure location

4 Seek Immediate Help & Advice

Contact support networks for guide and urgent assistance

- ✓ Reach out to digital security helplines or local HRD organizations
- ✓ Contact legal or technical experts if necessary
- ✓ Inform trusted colleagues or friends who can offer support

5 Stay Safe and Monitor

Take extra precautions and monitor for further threats.

- ✓ Limit online exposure by adjusting privacy settings
- ✓ Monitor accounts for further harassment or suspicious activity
- ✓ Follow up on any reports or complaints you have filed

What To Do If a Case Is Filed Against You?

Facing an FIR, legal notice, or summons under cyber laws can be frightening — especially for Human Rights Defenders whose work is already under scrutiny. However, panic can lead to mistakes. A calm and strategic response protects both you and your case.

Below is a step-by-step guide on how to respond safely and responsibly.

1 Do Not Delete Everything Immediately

Your first instinct may be to delete posts, messages, or accounts. However:

- Deleting content after a complaint may be interpreted as destruction of evidence.
- Authorities may already have screenshots or digital records.
- Sudden deletion may weaken your defense.

2 Preserve data

- Take screenshots of everything relevant.
- Preserve original posts and timestamps.

3 Seek Legal Protection

Provide your lawyer with:

- The FIR or notice (if available).
- Copies of posts in question.
- Any threatening messages you received.
- Background context of your work.

4 Do Not Give Statements Without Legal Advice

You may receive:

- A phone call from investigators.
- A request to "just come for questioning."
- Informal pressure to explain yourself.

Do not provide written or recorded statements without your lawyer present.

5 Inform Trusted Colleagues or Networks

Inform your organization ,trusted HRD networks ,legal advocacy groups or a family member

Public awareness can deter abuse of process.Colleagues can monitor your safety and networks can mobilize support if needed.

6 Consider Applying for Protective Legal Remedies

- Pre-Arrest Bail (Anticipatory Bail), Post-Arrest Bail, Protective Bail (Transit Bail)
- Writ Petition (Article 199 of the Constitution)
- Petition to Quash FIR
- Stay Order Against Harassment or Investigation Abuse
- Application for Return of Seized Devices
- Complaint Against Abuse of Authority

Many HRDs face legal intimidation. Respond Strategically, Not Emotionally. If a case is filed against you: do not panic, react impulsively or isolate yourself.

Reporting & Responding to Digital Threats

Document Everything Immediately

Before reporting or responding publicly, preserve evidence. Capture:

- Screenshots of messages, profiles, comments, and posts
- Full URLs of offending content
- Usernames and profile links
- Dates and times (including your time zone)
- Any prior interaction history

Secure Your Accounts

Before filing a complaint:

- Change your passwords immediately.
- Enable two-factor authentication (2FA).
- Review account recovery emails and phone numbers.
- Check for unknown login sessions.
- Inform trusted contacts not to click suspicious links sent from your account.
- If your account has been hacked, report it to the platform immediately.

Report to Authorities

In Pakistan, cybercrime complaints can be filed with the:

National Cyber Crime Investigation Agency

Sending an email to:
helpdesk@nccia.gov.pk

24/7 Helpline:1799

Online Complaint Portal:
https://complaint.nccia.gov.pk

Ministry of Human Rights Helpline 1099

You may:

- File an online complaint through the portal
- Visit the nearest NCCIA Cyber Crime office in person
- Call their helpline

Use Platform Reporting Mechanisms

In addition to filing with authorities:

- Report abusive accounts directly to the platform (Facebook, X, Instagram, etc.).
- Request removal of harmful content.
- Save confirmation emails of your reports.
- Platform reports create a documented trail of abuse.

Inform Trusted Networks

- If harassment is targeted and coordinated:
- Inform your organisation or HRD network like HRCP, Freedom Network, Digital Rights Foundation or PJN Digital Defender Portal.
- Alert digital rights organisations.
- Consider a collective response if safe.
- Public exposure of coordinated harassment sometimes discourages attackers — but this should be done carefully and strategically.

REMEMBER!

When responding to digital threats:

- ✓ Document first
- ✓ Secure your accounts
- ✓ Report strategically
- ✓ Seek legal advice if necessary
- ✓ Preserve evidence safely
- ✓ Protect your emotional well-being

PEACE AND
JUSTICE NETWORK
پیس اینڈ جسٹس نیٹ ورک پاکستان

CONSTITUTION OF PAKISTAN ARTICLE 25 (1)

EQUALITY OF CITIZENS

All citizens are equal before law and
are entitled to equal protection of law.

CONSTITUTION OF PAKISTAN ARTICLE 19

FREEDOM OF SPEECH & EXPRESSION

Every citizen shall have the right to
freedom of speech and expression.

DIGITAL RIGHTS ARE HUMAN RIGHTS

Every citizen in Pakistan has the right to privacy,
protection, safety, and freedom of expression.

PEACE & JUSTICE NETWORK

/PJNPakistan /PJNPakistan /PJNPakistanofficial www.pjn.org.pk contact@pjn.org.pk