DRF Submission to OHCHR: Protection of human rights defenders in the digital age

1. Legislative and regulatory measures

- **What impacts have recent trends in legislative and regulatory efforts at local, regional, and global levels – including, for example, on information integrity, online safety, and cybercrimse – had on the work and safety of HRDs offline and online?**

Human rights defenders (HRDs) are facing an increasingly challenging environment in their efforts to promote and protect human rights across regions. Civic space remains significantly constrained, and its current state is rated repressed for Pakistan[1], while several other countries in the Asia region are classified as obstructed, repressed, or closed[2]. Over time, many governments have expanded their control over online and offline spaces through broadly framed laws to suppress critical speech, restrict freedom, expand surveillance, and access information that can be used against HRDs. As a result, HRDs often operate in hostile environments where their work, particularly when it involves holding power holders accountable or advocating on sensitive issues, can expose them to threats, surveillance, censorship, imprisonment, and violence from both state and non-state actors.

The following legislative and regulatory measures illustrate how the legal framework increasingly affects the work and safety of HRDs;

Recent Local Legislative and Regulatory Trends

- In Pakistan, the Prevention of Electronic Crimes Act 2016 (“PECA”), a cybercrime framework enacted in light of the National Action Plan to counter terrorism[3], has been widely criticized for its negative impact on internet freedoms and digital rights. While the government maintained that PECA is aimed at combating cybercrimes and protecting cyberspace against threats to information integrity. However, its implementation over the past decade has revealed a pattern of its vague provisions being applied to restrict online expression and control content that is critical of state institutions, particularly against the government and armed forces. Various human rights observers[4], including a

[1] https://monitor.civicus.org/country/pakistan/
[2] https://monitor.civicus.org/search/countries/?territories=Asia&status=
[3] https://nacta.gov.pk/laws-policies/nap-2014/
[4] https://www.ifj.org/media-centre/news/detail/article/pakistan-peca-amendments-further-tighten-government-grip-on-digital-expression#:~:text=Since%20passing%20in%202016%2C%20the%20PECA%20has,government%20enforcing%20frequent%20shutdowns%20of%20online%20platforms.

former UN Special Rapporteur on the right to freedom of expression[5], criticized the Act[6] and its recent 2025 amendment for[7] its broadly framed offences, which are subject to generous interpretation by authorities, specifically against HRDs[8]. Out of the 26 criminal offences outlined in PECA, those relating to online speech have greatly impacted HRDs, state critics, and political opponents the most, mainly among these being Sections 10 (Cyber Terrorism), 11 (Hate Speech), 20 (Defamation)[9], and recently inserted 26-A (Fake News)[10] through the 2025 Amendment[11]. Though Section 20 was partly struck down by the Islamabad High Court[12] in 2022, on the grounds of unconstitutionality, it has nonetheless been upheld by the Lahore High Court[13]. However, the status of Section 20 remains unclear as it is pending before the Supreme Court[14], and similarly, the 2025 amendment has been challenged in Karachi[15], Lahore[16], Islamabad[17], and the Supreme Court[18]. Despite this, Sections 20[19] and 26-A[20] continue to be used in FIRs against HRDs and ordinary citizens to silence criticism of the government or state institutions. For instance, between 2025 and 2026, multiple HRDs were served notices or summoned for reporting on issues or posting content critical of state actions, with 689 cases registered under PECA between January and August 2025 alone[21], many targeting journalists for

---

5 https://www.ohchr.org/en/statements-and-speeches/2015/12/un-expert-urges-pakistan-ensure-protection-freedom-expression-draft?LangID=E&NewsID=16879

6 https://digitalrightsfoundation.pk/wp-content/uploads/2025/02/Bytes-Behind-Bars-Decoding-Pakistans-digital-expression-legislation.pdf

7 https://digitalrightsfoundation.pk/wp-content/uploads/2025/01/The-Prevention-of-Electronic-Crimes-Amendment-Act-2025-DRF-Analysis-and-Recommendations.pdf

8 https://www.iiu.edu.pk/wp-content/uploads/2024/05/ILR-Vol-7-Issue-2-Article-2-210524.pdf

9 https://bytesforall.pk/sites/default/files/CSO-criticism-on-PECB-2016_IssuePaper.pdf

10 https://digitalrightsfoundation.pk/probing-attacks-on-journalists-investigative-analysis-of-pecas-post-amendment-2025-cases/

11 https://www.na.gov.pk/uploads/documents/679255ee36f45_595.pdf

12 https://digitalrightsmonitor.pk/wp-content/uploads/2022/04/PFUJ-v-The-President-of-Pakistan-etc-WP-No-666-of-2022.pdf

13 https://sys.lhc.gov.pk/appjudgments/2022LHC1786.pdf

14 https://www.dawn.com/news/1872139

15 https://www.dawn.com/news/1891106#:~:text=The%20petitioners%20further%20argued%20that,ultra%20vires%20of%20the%20Constitution.

16 https://tribune.com.pk/story/2532581/lhc-ihc-take-up-pleas-against-peca

17 https://tribune.com.pk/story/2529266/ihc-acting-cj-takes-up-peca-plea

18 https://arynews.tv/peca-law-2025-sc-moved-against-controversial-amendments

19 https://cfj.org/wp-content/uploads/2023/10/Pakistan_PECA-Report_September-2023.pdf

20 https://digitalrightsfoundation.pk/probing-attacks-on-journalists-investigative-analysis-of-pecas-post-amendment-2025-cases/

21 https://www.hrw.org/world-report/2026/country-chapters/pakistan

online speech. A lower court also ordered the blocking of 27 YouTube channels[22] on the NCCIA's request for spreading anti-state content, and fake, misleading information. Most recently in 2026, human rights lawyers and activists Imaan Mazari and Hadi Ali Chattha were convicted to a combined 17 years' imprisonment[23] for online expression critical of state institutions, a decision condemned by many, including UN experts[24]. Such legal frameworks have established a pattern that creates an environment of fear, leading HRDs to self-censor as a precaution against legal repercussions. Consequently, civic space has been significantly constrained, limiting legitimate advocacy, dissent, and the documentation of human rights violations.

- The Punjab Defamation Act 2024[25], passed in May 2024 and applicable to the province of Punjab, is another legislation that presents significant threats to freedom of expression for HRDs in Pakistan[26]. The Act's emphasis on prosecuting defamation, particularly targeting "public officials," is an example of its authoritarian nature, potentially allowing the suppression of criticism directed at individuals associated with the government or other official institutions. The necessity of introducing this legislation is also questionable, given that existing frameworks, including PECA 2016[27], the PEMRA Ordinance 2002[28], and the Defamation Ordinance 2002[29], were already in place, raising concerns that the Act may primarily be passed with an intention to further centralize control and limit public scrutiny. However, the practical impact of this Act remains to be seen, as the legislation has been challenged at the Lahore High Court by Writ Petition No. 583648/2024[30] since its approval. Nevertheless, the overall structure of the Act already signals potential misuse against HRDs and ordinary citizens. By broadening the scope of "defamation" and "broadcasting" to include social media content, allowing legal action to be initiated without proof of actual damage, and imposing severe fines, a submission before the UN Human Rights Council[31] highlights that the Act can trigger fears of censorship, as the law authorities gain unchecked power to penalize online speech.

---

[22] https://www.dawn.com/news/1922836
[23] https://www.dawn.com/news/1968788
[24] https://www.ohchr.org/en/press-releases/2026/02/pakistan-un-experts-alarmed-conviction-imaan-mazari-hazir-and-hadi-ali
[25] https://punjablaws.punjab.gov.pk/uploads/articles/punjab-defamation-act-2024-pdf.pdf
[26] https://digitalrightsfoundation.pk/wp-content/uploads/2024/05/Comparison-and-Legal-Analysis-of-Punjab-Defamation-Bill-2024.pdf
[27] https://pakistancode.gov.pk/english/UY2FqaJw1-apaUY2Fqa-apaUY2Jvbp8%253D-sg-jjjjjjjjjjjj
[28] https://pakistancode.gov.pk/pdffiles/administrator0d8373dfae195c4de13b0bd012416abb.pdf#viewer.action=download
[29] https://pakistancode.gov.pk/english/UY2FqaJw1-apaUY2Fqa-apaUY2FwbZ8%3D-sg-jjjjjjjjjjjj
[30] https://www.dawn.com/news/1838774
[31] https://docs.un.org/en/A/HRC/59/NGO/57

- The right to privacy remains particularly vulnerable in Pakistan despite being constitutionally protected under Article 14[32], especially in digital spaces amid the state's ongoing attempts to exercise more control over the internet. Regardless of years of lobbying by digital rights groups on multiple drafts of the Personal Data Protection Bill (2018[33], 2020[34], 2021[35], and 2023[36]), no law has been enacted. This legal vacuum leaves HRDs and survivors without enforceable safeguards[37] governing how the data will be used, collected, stored, shared, or retained by state or private actors, which may risk misuse, unauthorized surveillance, and breaches of confidential communications. However, even if the law is enacted, questions about a rights-respecting data protection law remain, as legal analysts warn it has serious flaws[38]. Certain sections of the bill, such as Section 15(a)(viii), allow for exceptions in the processing of sensitive and critical personal data under court orders, and Section 29(6) introduces a public interest exception to data portability. While such exceptions are necessary for judicial procedures and public orders, they must align with the fundamental right to privacy, the right of information, and other necessary protocols. Otherwise could lead to the risk of exposing data of journalists, whistleblowers, researchers, academics, and non-governmental organizations[39], potentially threatening HRDs' security and confidentiality, along with impeding the advocacy work on accountability issues and sensitive matters. In this regard, a report to the UN General Assembly[40] also emphasized the need to protect sources and whistleblowers and urged states to prioritize disclosures made in the public interest over restrictive measures. Similarly, international best practice, reflected in the EU's General Data Protection Regulation ("GDPR")[41], allows data processing for only substantial public interest under Article 9(2)(g), emphasizing that appropriate safeguards should be in place. Moreover, data localisation requirements (Section 31) and cross-border transfer rules (Section 32), along with broad exemptions for data collection related to research and statistics (Section 34(2)(f)), could also lead to exposing data to the government and restrict the use of cloud services and secure communication

[32] https://www.pakistani.org/pakistan/constitution/
[33] https://digitalrightsfoundation.pk/wp-content/uploads/2018/08/DP-Comments-Brief-Final-8.8.18-1.pdf
[34] https://digitalrightsfoundation.pk/wp-content/uploads/2020/05/PDPB-2020_-Final-Analysis_05.05.2020-1.pdf
[35] https://digitalrightsfoundation.pk/wp-content/uploads/2021/09/PDPB-2021-Submission-by-DRF.pdf
[36] https://digitalrightsfoundation.pk/wp-content/uploads/2023/07/Legal-Analysis-Statement-on-PDPB-July-2023.pdf
[37] https://www.thefridaytimes.com/11-Dec-2025/data-privacy-peril-pakistan-s-legal-vacuum-consequences?utm_source=chatgpt.com
[38] https://digitalrightsfoundation.pk/wp-content/uploads/2023/07/Legal-Analysis-Statement-on-PDPB-July-2023.pdf
[39] https://bytesforall.pk/sites/default/files/CSO-criticism-on-PECB-2016_IssuePaper.pdf
[40] https://docs.un.org/en/A/70/361
[41] https://gdpr-info.eu/art-9-gdpr/

channels relied upon by civil society actors for international collaboration. Additionally, the limited independence of the Data Protection Commission (Sections 35, 37, 43, and 47) weakens its capacity to effectively oversee data protection. To sum up, in its current form, the draft falls short in addressing data safety concerns due to weak governance, vague definitions, diluted data subject rights, and expansive exemptions. This gap exposes citizens to unchecked data use, surveillance, and discriminatory profiling, raising critical concerns about how digitalization impacts the protection and realization of human rights, particularly for HRDs.

- With increasing internet penetration and expanding digital infrastructure, Pakistan passed the Digital Nation Act (DNA) 2025[42] to unify the digital ecosystem that integrates state institutions and citizens through a centralized framework of digital identities and data repositories. While designed to streamline governance, civil society[43] has raised concerns that this integration has exacerbated concerns of unchecked state overreach. By centralizing citizens' digital identities and governance data without legal safeguards, the framework risks mass surveillance and data misuse, which threatens the rights to privacy, autonomy, and equality before the law protected under Articles 4, 9, 14, and 25 of the Constitution of Pakistan[44]. The DNA grants broad powers to the Pakistan Digital Authority, constituted under the DNA, to integrate and share citizen data across institutions. Without judicial authorization or independent oversight, this centralisation opens the door to near constant state surveillance under the guise of digital efficiency. Existing practices already illustrate these dangers. For instance, section 54(1) of the Pakistan Telecommunication (Re-organization) Act, 1996[45] empowers the Federal Government to authorize any person to “intercept calls and messages or to trace calls through any telecommunication system” in the interest of national security. Furthermore, the Fair Trial Act, 2013[46], allows security agencies to seek a judicial warrant to monitor private communications of terror suspects. Similarly, the Removal and Blocking of Unlawful Online Content (Procedure, Oversight and Safeguards) Rules[47], 2021 mandate social media companies to provide decrypted information to the relevant wing established under PECA. Moreover, the telecom regulator’s installation of a Lawful

[42] https://pakistancode.gov.pk/pdffiles/administrator2c2fd2fe7da1a657c40589a0705b3e20.pdf

[43] https://digitalrightsfoundation.pk/wp-content/uploads/2026/01/The-Cost-of-Going-Digital_-Evaluating-Rights-Risks-in-Pakistans-Digital-Governance.pdf

[44] https://www.pakistani.org/pakistan/constitution/

[45] https://pakistancode.gov.pk/pdffiles/administratorcf6de2451af9e9d016e5fef2ac7e1562.pdf#viewer.action=download

[46] https://pakistancode.gov.pk/pdffiles/administrator289aee517e7b8512e341194f9e846738.pdf#viewer.action=download

[47] https://moitt.gov.pk/SiteImage/Misc/files/Removal%20Blocking%20of%20Unlawful%20Online%20Content%20Rules%202021.PDF

Intercept Management System (LIMS)[48] allows state agencies to monitor users' calls, messages, and internet activity without transparent legal oversight, only exemplifying how technological interventions can outpace accountability mechanisms. By merging identity, financial, and social data, the state gains unprecedented visibility into citizens' lives, with little regard for consent, purpose, or data retention. This unchecked surveillance operating without transparent limits affects everyone but hits human rights defenders and journalists the hardest[49], fostering fear, intimidation, and self-censorship. The media faces censorship, websites and YouTube channels are blocked, and reporters are geo-tracked, further exacerbating their experience as front-line defenders. The 2025 World Press Freedom[50] ranking places Pakistan at 158th of 180 countries, underscoring the dangers that vulnerable groups face daily. Without a comprehensive data protection law, such initiatives normalize intrusion, erode public trust, and enable surveillance of dissent, journalists, and marginalized communities.

- Amendment to the Official Secrets Act (OSA), 1923[51], in 2023 has been widely criticised[52] for providing excessive powers to intelligence agencies, thereby strengthening this draconian law to pose further risks to HRDs. The meaning of "enemy" has been expanded by the amendment, which now places a liability of spying on a person who directly or indirectly works with a foreign power, agent, organization, or association, without even defining what collaboration can be considered against the State's security and interest. Many human rights groups criticized the amendment and called it a blatant violation of constitutional rights and international human rights[53]. Irrespective of the intent of the legislature behind inserting this amendment, the law has the potential to silence HRDs and create a holistic environment for HRDs to work. Parallel to this, the Anti-Terrorism Act, 1997 (ATA), has also been frequently criticized for being used against HRDs due to its excessively broad, ambiguous, and often misused definition of "terrorism." The Supreme Court has ordered a narrow reading of offences under the ATA in a landmark judgment in Ghulam Hussain v. the State[54].

- In addition to laws used to restrict the rights and freedoms of HRDs, provisions of the Pakistan Penal Code (PPC) 1860[55] have increasingly been invoked against individuals

---

[48] https://www.dawn.com/news/1843299

[49] https://www.bytesforall.pk/post/pakistan-proposed-peca-amendment-and-digital-nation-pakistan-bill-threaten-digital-rights

[50] https://observerdiplomat.com/pakistan-ranked-158-of-180-in-the-world-press-freedom-index-2025/

[51] https://pakistancode.gov.pk/pdffiles/administrator46c9a3c62acc16428e73999e7d30ba2a.pdf

[52] https://www.iiu.edu.pk/wp-content/uploads/2024/05/ILR-Vol-7-Issue-2-Article-2-210524.pdf

[53] https://rcilhr.com/the-legality-of-trying-civilians-in-military-courts-under-pakistani-law-and-constitution/

[54] https://www.supremecourt.gov.pk/downloads_judgements/crl.a._95_2019.pdf

[55] https://pakistancode.gov.pk/pdffiles/administratord5622ea3f15bfa00b17d2cf7770a8434.pdf#viewer.action=download

engaged in reporting, advocacy, or expression on politically or socially sensitive issues. The PPC contains several broadly worded offences carrying severe penalties, ranging from imprisonment to capital punishment. These include, inter alia, mainly sedition under section 124-A, criminal defamation under section 500, and blasphemy-related offences under sections 295 (a), (b), (c) and 298 (a), (b), (c). The vague and expansive wording of these provisions, particularly relating to alleged insults against the state, religious sentiments, or public order, creates significant scope for misuse[56]. As per the Digital Rights Foundation[57], many journalists frequently face coordinated hate campaigns on Twitter, TikTok, Facebook, and YouTube over their reporting on blasphemy cases, showing a trend where such laws are increasingly used to target HRDs reporting on sensitive issues. Similarly, the Human Rights Commission of Pakistan reported[58] many cases where these sections were employed to initiate criminal proceedings against HRDs whose work involves criticism of government actions, or reporting on matters relating to religion, governance, or public policy. This evident abuse and violence under such legal frameworks have routinely put the security of journalists, human rights defenders, and the public at risk. As a result, the space for expressing opinions, accessing information, and carrying out accountability work has visibly shrunk for HRDs[59].

Regional/Global Legislative and Regulatory Trends

- In 2023, India passed the Digital Personal Data Protection (DPDP) Act[60], which replaces the data protection regime under the Information Technology Act, 2000[61], and establishes a national framework for individuals' digital personal data. While this legislation is marked as India's first-ever privacy act, there has been a strong pushback[62]

---

56 https://hrcp-web.org/hrcpweb/wp-content/uploads/2020/09/2022-Freedom-of-peaceful-assembly-in-Pakistan.pdf

57 https://digitalrightsfoundation.pk/wp-content/uploads/2024/12/Gendered-Online-Hate-in-Pakistan-Right-Wing-Religious-Campaigns-Against-Women-Journalists.pdf

58 https://hrcp-web.org/hrcpweb/wp-content/uploads/2020/09/2022-Freedom-of-peaceful-assembly-in-Pakistan.pdf

59 https://hrcp-web.org/hrcpweb/wp-content/uploads/2020/09/2022-Joint-submission-for-Pakistans-fourth-UPR.pdf

60 https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf

61 https://eprocure.gov.in/cppp/rulesandprocs/kbadqkdlcswfjdelrquehwuxcfmijmuixngudufgbuubgubfugbububjxcgfvsbdihbgfGhdfgFHytyhRtMjk4NzY=

62 https://www.dw.com/en/india-data-law-surveillance-privacy-big-tech-data-protection-press-freedom/a-74923737

against its implications for human rights. As per the Internet Freedom Foundation[63], the DPDP Act, and its implementing DPDP Rules, 2025[64], instead of protecting citizens' data rights, have created barriers to transparency and individual freedoms with broad exceptions. The government can now get personal data from any data fiduciary or intermediary[65] on broad grounds such as the "sovereignty and integrity of India" or "security of the state," without clear safeguards, transparency obligations, or judicial oversight. In addition, amendments linked to the Act allow authorities to deny disclosure of personal information of public officials[66] under the Right to Information Act, 2005[67], even for a larger public interest. Such provisions risk creating barriers for HRDs to investigative work into corruption, restricting access to information about public officials' misconduct, and increasing concerns related to surveillance and data-based targeting of activists.

- In Sri Lanka, the enactment of the Online Safety Act (OSA) 2024[68] has undermined human rights[69] and led to a shrinking civic space[70]. The law criminalizes "prohibited statements"[71] that are deemed to promote ill-will or threaten national security, along with vaguely defined categories of prohibited content, disproportionate penalties for online speech[72], and the establishment of an Online Safety Commission with broad powers[73]. The Global Network Initiative[74] emphasises that if these provisions are left unaddressed, then it will risk undermining Sri Lankans' ability to freely express themselves, access information, and participate in democratic debate online. However, this risk is not hypothetical: authorities[75] and parliamentarians[76] have invoked the Act to accuse individuals of spreading "false information" or making "defamatory or derogatory

63 https://internetfreedom.in/iffs-initial-statement-on-the-notification-of-the-digital-data-protection-rules-2025/
64 https://www.dpdpa.com/dpdparules.html
65 https://www.thenewsminute.com/news/data-protection-rules-2025-critics-say-it-grants-unchecked-power-to-the-state
66 https://www.thenewsminute.com/news/data-protection-rules-2025-critics-say-it-grants-unchecked-power-to-the-state#:~:text=A%20key%20provision%2C%20Rule%2023,Board%2C%20data%20fiduciaries%20or%20intermediaries
67 https://cic.gov.in/sites/default/files/RTI-Act_English.pdf
68 https://www.parliament.lk/uploads/acts/gbills/english/6311.pdf
69 https://globalnetworkinitiative.org/gni-urges-human-rights-reforms-to-sri-lankas-online-safety-act/
70 https://www.icj.org/wp-content/uploads/2025/09/ICJ_Online-Safety-Act_Submission.pdf
71 https://www.icj.org/wp-content/uploads/2025/09/ICJ_Online-Safety-Act_Submission.pdf
72 https://globalnetworkinitiative.org/gni-urges-human-rights-reforms-to-sri-lankas-online-safety-act/
73 https://www.icj.org/wp-content/uploads/2025/09/ICJ_Online-Safety-Act_Submission.pdf
74 https://globalnetworkinitiative.org/gni-urges-human-rights-reforms-to-sri-lankas-online-safety-act/
75 https://www.dailymirror.lk/top-story/First-application-under-Online-Safety-Act-filed-before-Court/155-280187?utm_source=chatgpt.com
76 https://www.dailymirror.lk/breaking-news/Court-issues-restraining-order-over-defamation-against-MP-Mujibur/108-311500

statements." If such application of the law continues, it will expose HRDs to arbitrary enforcement, increase the risk of censorship, discourage public discourse on matters of public interest, and impose impermissible restrictions on freedom of expression.

- In Bangladesh, the Cyber Security Act (CSA) 2023[77], which replaced the Digital Security Act (DSA) 2018[78], has been widely criticized as a repackaging of repression[79]. The law grants authorities sweeping powers to search, arrest, detain, and seize devices without adequate safeguards for data privacy. Within six months of its enactment, Amnesty International found[80] media reports to have documented at least ten cases targeting individuals for allegedly defaming the prime minister or other government officials. Such legal frameworks risk being used against the critics[81], leaving human rights defenders vulnerable to surveillance and arbitrary enforcement.

- **What legal or regulatory instruments and institutional procedures are commonly used to restrict the rights to freedom of expression, association, and privacy of HRDs online?**

HRDs increasingly depend on digital platforms for advocacy, organization, and communication. Protecting their online rights is thus essential. Yet many governments have adopted broad laws and vague policies that restrict online freedoms only because these HRDs issued a *"prohibited statement",* or spread *"fake news"*. In light of the same, the UN Special Rapporteur on Freedom of Expression[82] has also warned that one of the worst threats to free speech is the criminalization of online criticism of government, religion, or other public institutions. In practice, HRDs face targeting through various laws and institutional procedures that censor dissent and infringe upon their fundamental rights in online spaces.

Legal Instruments And Institutional Procedures

Several laws and institutional procedures have been used to limit HRDs' online rights:

1. **<u>Cybersecurity/Repressive Cybercrime Laws</u>**

---

77 https://legislativediv.portal.gov.bd/sites/default/files/files/legislativediv.portal.gov.bd/page/74e04fe7_3a20_4636_8e6e_e8d52c3f5182/Cyber%20Secrity.pdf

78 https://www.icnl.org/wp-content/uploads/Digital-Security-Act-2018-English-version.pdf

79 https://www.amnesty.org/en/wp-content/uploads/2024/08/ASA1383322024ENGLISH.pdf

80 https://www.amnesty.org/en/latest/news/2024/08/bangladesh-interim-government-must-restore-freedom-of-expression-in-bangladesh-and-repeal-cyber-security-act/

81 https://cfj.org/wp-content/uploads/2024/11/Bangladesh-ICT-Act-Report_November-2024-1.pdf

82 https://www.ohchr.org/en/press-releases/2018/06/landmark-report-un-expert-urges-governments-and-internet-firms-ensure#:~:text="The%20worst%20threats%20include%20the,such%20decisions%20require%2C"%20said%20Mr

- Many countries have enacted cybersecurity laws with vague provisions that restrict HRDs' rights to freedom of expression, association, and privacy. For example, Pakistan's Prevention of Electronic Crimes Act (PECA, 2016)[83], initially enacted to counter cybercrimes, now penalizes broad online offences such as "fake news" and "defaming" state institutions, with harsh penalties. Furthermore, the 2025 amendments[84] to the PECA 2016 have drawn strong criticism from civil society. Rights groups[85] warn that the changes significantly expand authorities' powers to monitor and restrict online expression. The act has been used to suppress freedom of speech under the guise of combating fake news, cybercrime, and misinformation[86].
    - In January 2026, two well-known human rights lawyers, Imaan Mazari and Hadi Ali Chattha[87], were convicted under the PECA 2016 for sharing social-media posts. The Islamabad district court sentenced them under sections 9 (glorification of an offence), 10 (cyberterrorism), and 26-A (fake news) of the Act, each for a total of 17 years in prison, with the longest term being 10 years for the charge of cyberterrorism. UN experts[88] described the verdicts as alarming, emphasizing that freedom of expression should not be equated with terrorism. This case highlights how vaguely defined online crimes can be leveraged to impose severe penalties on what would normally be considered routine political critique.

- The Sri Lankan parliament enacted the new Online Safety Act (OSA) 2024[89] on 24th January 2024, introducing far-reaching restrictions on digital expression. Despite amendments introduced in August, concerns remained. Vaguely worded offences and the broad powers granted to authorities risk being used to restrict freedom of expression. There were also fears that the law could be applied to suppress dissent.
    - According to Amnesty International[90], the Act establishes an Online Safety Commission with wide powers. It can determine what constitutes a "prohibited statement" and order service providers to remove content or disable access to

[83] https://pakistancode.gov.pk/english/UY2FqaJw1-apaUY2Fqa-apaUY2Jvbp8%253D-sg-jjjjjjjjjjjj
[84] https://www.na.gov.pk/uploads/documents/679255ee36f45_595.pdf
[85] https://www.amnesty.org/en/latest/news/2025/01/pakistan-authorities-pass-bill-with-sweeping-controls-on-social-media/
[86] https://www.hrw.org/news/2022/02/28/pakistan-repeal-amendment-draconian-cyber-law
[87] https://www.reuters.com/world/asia-pacific/pakistan-sentences-human-rights-activist-17-years-over-anti-state-posts-2026-01-24/
[88] https://www.ohchr.org/en/press-releases/2026/02/pakistan-un-experts-alarmed-conviction-imaan-mazari-hazir-and-hadi-ali#:~:text="Lawyers%2C%20like%20other%20individuals%2C%20are
[89] https://www.reuters.com/world/asia-pacific/sri-lanka-votes-new-law-regulate-online-content-2024-01-24/
[90] https://www.amnesty.org/en/latest/news/2024/01/sri-lanka-online-safety-act-major-blow-to-freedom-of-expression/

individuals. Moreover, the Act also prohibits the "communication of a false statement" where such a statement is deemed to threaten national security, public health, or public order. The powers granted to the commission are broad and lack clear safeguards, with limited clarity on definitions and independent oversight.

- Similarly, Bangladesh has enacted various laws that restrict human rights defenders (HRDs), journalists, lawyers, and political dissidents. The Digital Security Act was enacted in 2018 (now repealed) and was presented by the Bangladeshi government as a measure that would prevent arbitrary arrests[91] under the Information and Communication Technology (ICT) Act 2006. However, as Human Rights Watch noted[92], the Act strengthened state control over online expression. The law criminalizes "propaganda or campaign against the liberation war, the spirit of the liberation war, the father of the nation, the national anthem or the national flag," with penalties that include life imprisonment. Such provisions have been widely criticised as disproportionate and as further tightening restrictions on the freedom of expression of the HRDs and others.

    - DSA was repealed on August 7, 2023, and replaced by the Cyber Security Act 2023. The Cyber Security Act (CSA) 2023 is a continuation of successive repressive laws in Bangladesh. These legislative measures have repeatedly enabled the state to intensify its crackdown on civic space and restrict the enjoyment of human rights. As noted by Amnesty International[93], the Act reflects an ongoing pattern of using digital security legislation to curb dissent and limit fundamental freedoms.
    - As per Amnesty International's analysis of CSA 2023[94], out of 62 provisions in the DSA 2018, 28 were retained verbatim, 25 were carried over with minor changes, such as modifications to terminology or sentencing, and 5 were retained with procedural adjustments. The CSA introduced only one new provision, creating an offence for filing false cases. In total, 58 of the 59

---

91 https://www.hrw.org/report/2018/05/10/no-place-criticism/bangladesh-crackdown-social-media-commentary

92 https://www.hrw.org/news/2019/05/17/bangladesh-new-arrests-over-social-media-posts#:~:text=The%20ICT%20Act%20was%20widely,curbing%20lawful%20criticism%20and%20dissent

93 https://www.amnesty.org/en/latest/news/2024/08/bangladesh-interim-government-must-restore-freedom-of-expression-in-bangladesh-and-repeal-cyber-security-act/

94 https://www.amnesty.org/en/documents/asa13/8332/2024/en/

provisions in the CSA were inherited from the DSA, either unchanged, slightly modified, or with procedural alterations.

- One such case which exemplifies the blatant consequences of CSA is the event of how, on 15 March 2025, the human rights defender Nahid Hassan Knowledge's[95] home in Chilmari was raided by the Detective Branch police from Kurigram in an attempt to arrest him. Authorities have filed a First Information Report (FIR) against him, including charges under the Cyber Security Act for allegedly hurting religious sentiments.

2. Data Protection Laws In The Age of Increasing Surveillance

- India's Digital Personal Data Protection Act (DPDPA), 2023[96], was enacted on August 11, 2023. It aims to protect privacy but includes broad governmental power[97]. Security agencies can demand any individual's data[98] from platforms for vague reasons, e.g., "sovereignty", "security of the state." Critics warn that this grants the state "unchecked power" to surveil citizens and stifle dissent. Civil society groups and activists[99] note that the DPDA Rules[100] enacted in 2025 even bar the disclosure of public officials' personal information under RTI.

    - Moreover, Indian HRDs and journalists have already faced digital surveillance abuses. Investigations by Amnesty[101] have noted that state actors repeatedly deployed NSO Group's Pegasus spyware against Indian journalists, lawyers, and activists. Following revelations from the Pegasus Project, the Supreme Court of India[102] established a technical committee to investigate abuses involving the spyware. In 2022, the committee completed its investigation, but the findings

---

95 https://www.frontlinedefenders.org/ar/case/human-rights-defender-nahid-hasan-knowledge-charged-under-cyber-security-act-hurting-religious#:~:text=Will%20they%20not%20be%20arrested,3.

96 https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf

97 https://thewire.in/rights/unchecked-powers-to-govt-new-barriers-to-transparency-iff-on-digital-personal-data-protection-act

98 https://www.thenewsminute.com/news/data-protection-rules-2025-critics-say-it-grants-unchecked-power-to-the-state#:~:text=A%20key%20provision%2C%20Rule%2023,Board%2C%20data%20fiduciaries%20or%20intermediaries

99 https://frontline.thehindu.com/social-issues/social-justice/dpdp-act-vs-rti-2026/article70679578.ece

100 https://www.dpdpa.com/dpdparules.html

101 https://www.amnesty.org/en/latest/news/2023/10/global-india-apple-notifications-highlight-the-unabated-threat-of-unlawful-targeted-surveillance/#:~:text="This%20latest%20round%20of%20Apple,be%20yet%20another%20surveillance%20scandal

102 https://www.theguardian.com/news/2021/oct/27/indian-supreme-court-orders-inquiry-into-states-use-of-pegasus-spyware

have not been made public. The court also noted that Indian authorities did not cooperate[103] with the committee during its inquiries.

- Bangladesh enacted its first Personal Data Protection Ordinance in 2025. Rights groups[104] say it contains broad exemptions that would shield law enforcement and intelligence from accountability. Under the PDPO, authorities could collect, use, and retain personal data without the usual purpose or consent limits, culminating in state-sponsored surveillance and human rights violations.

    - In January 2023, reports[105] emerged that Bangladesh's government purchased Israeli Pegasus spyware for USD 6 million. Although officials denied it, activists and opposition leaders fear the device is being used to monitor citizens. Transparency groups warned that using such spyware would "undermine the privacy" and free expression of individuals.

3. Defamation laws

- Pakistan's use of criminal defamation laws has increasingly restricted the exercise of freedom of expression. Sections 499 and 500[106] of the Pakistan Penal Code, along with Section 20[107] of the Prevention of Electronic Crimes Act, 2016 (PECA), criminalize defamation and have been invoked against critics of the state and military[108].

    - The Islamabad High Court[109] (IHC) has criticized the Federal Investigation Agency (FIA) for misusing its powers under Section 20 of PECA 2016, i.e., criminal defamation. The court noted that the agency had issued notices and carried out arrests targeting journalists and government critics, reports[110] also indicate that between 2019 and 2021, at least 23 journalists were targeted under PECA. A recent three-part series in Dawn[111], a credible news source in Pakistan,

---

103 https://www.ndtv.com/india-news/pegasus-case-29-phones-examined-malware-in-5-but-no-conclusive-proof-that-it-had-the-spyware-says-supreme-court-3284651

104 https://www.hrw.org/news/2025/02/25/joint-statement-emerging-digital-laws-bangladesh#:~:text=through%20broad%20exemptions%20for%20law,controllers%20and%20processors%20in%20a

105 https://www.arabnews.com/node/2232246/world#:~:text=The%20Israeli%20daily%20Haaretz%20reported,country%20in%20June%20last%20year

106 https://www.pakistani.org/pakistan/legislation/1860/actXLVof1860.html

107 https://pakistancode.gov.pk/english/UY2FqaJw1-apaUY2Fqa-apaUY2Jvbp8%253D-sg-jjjjjjjjjjjj

108 https://mediamatters.pk/wp-content/uploads/2022/10/Criminalising-Defamation.pdf

109 https://digitalrightsmonitor.pk/no-hesitation-in-calling-peca-a-draconian-law-says-islamabad-high-court/

110 https://www.aljazeera.com/news/2021/11/2/pakistan-journalists-targeted-cyber-crime-law-press-freedom

111 https://www.dawn.com/news/1726162

titled Project PECA, described the law as "*an effective weapon in the hands of the state to harass, intimidate and silence critics*." These developments highlight the chilling effect of PECA on independent reporting and civic space.

- Similarly, India has long criminalised defamation under the Indian Penal Code, where Sections 499 and 500 defined defamation and prescribed punishment. The colonial-era code has since been replaced[112] by the Bharatiya Nyaya Sanhita (BNS) 2023[113], which largely retains the same structure. Moreover, the Code of Criminal Procedure, 1973, and the Indian Evidence Act, 1872, were also replaced[114] by the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS) and the Bharatiya Sakshya Adhiniyam, 2023 (BSA).

    - Under Section 356 of the BNS, defamation occurs when a person makes, publishes, or circulates any statement, spoken, written, or visual, that harms another person's reputation. While defamation laws are intended to protect individuals from false and damaging statements, criminal defamation provisions have repeatedly raised concerns among rights groups[115]. For example, a court of first instance in Gujarat sentenced independent investigative journalist Ravi Nair[116] to one year in prison. The conviction arose from a criminal defamation case filed by Adani Enterprises Limited, part of the vast conglomerate owned by billionaire Gautam Adani.

3. Institutional Censorship and Enforcement Procedures

- Institutional procedures curbing the freedom of journalists, activists, and human rights defenders are also on the rise, with content takedowns, summons, arrests, and internet shutdowns creating a chilling effect on expression and association. For instance, India's Ministry of Electronics & IT (MeitY) regularly orders online content to be blocked under the IT Act. For instance, in February 2024, MeitY instructed social media platforms to block 177[117] accounts linked to the farmers' protests.

---

112 https://www.ndtv.com/india-news/colonial-era-ipc-out-new-criminal-laws-take-effect-today-10-points-6005426

113 https://www.mha.gov.in/sites/default/files/250883_english_01042024.pdf

114 https://rsilpak.org/2024/rewriting-criminal-law-in-india/

115 https://pucl.org/manage-press-stateme/pucl-condemns-the-conviction-of-medha-patkar-for-defamation-repeal-defamation-in-bharatiya-nyaya-sanhita-bns-as-a-colonial-vestige/#:~:text=SLAPPS%20suits%2C%20world-wide%2C,courageous%20struggle%20against%20arbitrary%20power.

116 https://www.newslaundry.com/2026/02/11/what-did-ravi-nair-tweet-about-adani-to-land-a-prison-sentence-and-a-fine

117 https://www.hindustantimes.com/india-news/amid-farm-protest-it-ministry-blocks-177-accounts-links-101708366564358.html

    - Indian state authorities routinely suspend Internet and mobile data to stifle dissent. According to Amnesty International[118], 40 shutdowns across India in 2024, from Kashmir to Kerala, were often imposed by district magistrates under the Telegraph Act or the Disaster Management Act. These shutdowns prevent HRDs from communicating and accessing information during protests or civil unrest, functioning as a blunt censorship tool.

- Similarly, Pakistan's Telecommunications Authority can unilaterally remove or block online content it deems unlawful, e.g., content that is against Islam, the integrity of the state, or public order. The Authority is empowered to block online content under Section 37(1) of the PECA, 2016, and Removal and Blocking of Unlawful Online Content (Procedure, Oversight and Safeguards) Rules 2021[119]. For example, in June 2025, a court in Islamabad[120], on the request of the National Cyber Crime Investigation Agency, ordered the blocking of 27 YouTube channels. The channels were accused of spreading "false and anti-state" content.

    - Additionally, Pakistan's authorities frequently disrupt[121] internet access to curb dissent[122]. The government often invokes emergency provisions, such as section 54 of the Pakistan Telecommunication (Re-organization) Act[123], 1996, to block mobile networks. Moreover, the Ministry of Information Technology and Telecommunication has further authorised the Inter-Services Intelligence (ISI) through a notification[124] under section 54 of the act to intercept and trace calls in the interest of national security. Rights activists[125] warn that such broad surveillance powers, exercised with limited transparency, risk undermining privacy and freedom of expression online.

---

118 https://www.amnesty.org/en/location/asia-and-the-pacific/south-asia/india/report-india/#:~:text=According%20to%20the%20Software%20Freedom,government%20jobs%20and%20higher%20studies

119 https://moitt.gov.pk/SiteImage/Misc/files/Removal%20Blocking%20of%20Unlawful%20Online%20Content%20Rules%202021.PDF

120 https://www.dawn.com/news/1922836

121 https://www.dawn.com/news/1752051

122 https://www.hrw.org/news/2024/12/12/dangerous-digital-crackdown#:~:text=The%20new%20proposals%20come%20in,and%20order%20and%20curbing%20misinformation

123 https://khalidzafar.com/wp-content/files_mf/1527082753PakistanTelecomReorganizationAct1996.pdf

124 https://www.dawn.com/news/1844810?fbclid=IwY2xjawQXgmFleHRuA2FlbQIxMABicmlkETFZUE1qQUZGVDVBVEdJQzg2c3J0YwZhcHBfaWQQMjIyMDM5MTc4ODIwMDg5MgABHnq06x08NRe59a_yzyOY85jVFOJosCNJk50Efn_Re4TaNmMwsoo3GtlCu0an_aem_NBKOCqE31GvrWKZo_tsWlg

125 https://www.arabnews.pk/node/2546556/pakistan

- **How have legislative and regulatory efforts in one country or region impacted similar legal and regulatory measures in other countries or regions?**

Legislative and regulatory efforts in one country or region frequently influence other jurisdictions through regulatory diffusion or policy transplantation, where legal frameworks travel across borders and serve as models, benchmarks, or cautionary examples for reform.

- A leading example is the EU's GDPR, which established a comprehensive and rights-based framework for personal data protection. The GDPR introduced enforceable rights for individuals, strict consent requirements for data processing, accountability obligations for organizations, and strong penalties for non-compliance. Because of its global influence, the GDPR has become a benchmark for privacy legislation worldwide. Likewise, Pakistan's proposed Personal Data Protection Bill Drafts, including Draft 2018[126], Draft 2020[127], Draft 2021[128], and Draft 2023[129] clearly reflect GDPR-inspired principles, including lawful and consent-based data processing, data minimization, purpose limitation, protection of sensitive personal data, data breach notification requirements, and the establishment of an oversight authority. Although the Bill remains pending, its structure demonstrates how European regulatory standards have directly influenced Pakistan's legislative drafting process and modernization of digital governance.
- The influence of GDPR and other similar benchmark laws/policies also come with an economic incentive. Countries engaging with European markets are incentivized to adopt comparable data protection standards to facilitate trade, digital services exports, foreign direct investment, and international cooperation.
- The GDPR's ripple effect is visible worldwide, including in Brazil, India, and Kenya. Brazil's LGPD (Lei Geral de Proteção de Dados, 2018)[130] draws on GDPR principles of consent, transparency, and data subject rights while unifying previously fragmented statutes. India's Digital Personal Data Protection Act, 2023[131] partially adopts GDPR-style rules for consent, purpose limitation, and obligations for data fiduciaries, with

[126] https://digitalrightsfoundation.pk/wp-content/uploads/2018/08/DP-Comments-Brief-Final-8.8.18-1.pdf
[127] https://digitalrightsfoundation.pk/wp-content/uploads/2020/05/PDPB-2020_-Final-Analysis_05.05.2020-1.pdf
[128] https://digitalrightsfoundation.pk/wp-content/uploads/2021/09/PDPB-2021-Submission-by-DRF.pdf
[129] https://digitalrightsfoundation.pk/wp-content/uploads/2023/07/Legal-Analysis-Statement-on-PDPB-July-2023.pdf
[130] https://www.gov.br/anpd/pt-br/centrais-de-conteudo/brazilian-data-protection-law.pdf
[131] https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf

penalties for non-compliance and powers for urgent remedial measures. Kenya's Data Protection Act (2019)[132] also mirrors certain GDPR provisions on accountability, data security, and enforcement, though adapted to local administrative and legal contexts. Each of these frameworks incorporates some core GDPR elements illustrating how legislation in one jurisdiction can catalyze global regulatory convergence while being tailored to local institutional contexts.

International Spread Of Security-Driven Cyber Governance Models

- In parallel with rights-based diffusion, Pakistan's regulatory landscape also reflects the international spread of security-driven cyber governance models. The Prevention of Electronic Crimes Act (PECA), 2016[133] embodies a state-centric approach influenced by global counter-terrorism frameworks and cybersecurity narratives. While such frameworks are often justified as necessary responses to cyber threats, they can also expand state oversight of digital spaces and influence how online expression is governed. This evolving cybercrime framework, particularly through amendments to PECA, illustrates how legal mechanisms can gradually expand state authority over digital spaces. These changes have significant implications for journalists, activists, and human rights defenders (HRDs) who rely on online platforms to document abuses and mobilize public awareness. Similar legislative trajectories are increasingly visible in neighboring countries, suggesting a pattern of regional regulatory convergence.
- In Sri Lanka, the adoption of the Online Safety Act (OSA), 2024[134] grants a government-appointed commission extensive authority to regulate and remove "prohibited" online content. Although framed as a response to online harms, rights groups have warned that the law may be used to suppress dissent, particularly following the significant role social media played during the 2022 protest movement.
- A comparable pattern has emerged in Bangladesh. The replacement of the widely criticized Digital Security Act (DSA)[135] with the Cyber Security Act[136] has not significantly altered the restrictive nature of the legal framework and has been widely criticized as a repackaging of earlier

[132] https://www.kentrade.go.ke/wp-content/uploads/2022/09/Data-Protection-Act-1.pdf
[133] https://pakistancode.gov.pk/pdffiles/administrator6a061efe0ed5bd153fa8b79b8eb4cba7.pdf
[134] https://www.reuters.com/world/asia-pacific/sri-lanka-votes-new-law-regulate-online-content-2024-01-24/
[135] https://www.icnl.org/wp-content/uploads/Digital-Security-Act-2018-English-version.pdf
[136] https://legislativediv.portal.gov.bd/sites/default/files/files/legislativediv.portal.gov.bd/page/74e04fe7_3a20_4636_8e6e_e8d52c3f5182/Cyber%20Secrity.pdf

repressive provisions. The law grants authorities broad powers to search, arrest, detain, and seize digital devices without adequate safeguards for data privacy and due process. Many of its provisions replicate those of earlier legislation and have historically been used to initiate legal proceedings against journalists, activists, and human rights defenders.

- Taken together, these developments demonstrate how cyber laws across South Asia increasingly reflect a regional pattern of regulatory borrowing, where governments adopt similar legal frameworks to control online spaces. For HRDs, this ripple effect has significant implications, as expanding cybercrime and online safety legislation can create legal risks for digital advocacy, limit the ability to document human rights violations, and contribute to a broader chilling effect on freedom of expression across the region.
- Regional developments further illustrate how restrictive digital governance practices can spread beyond legislative frameworks into direct control of digital infrastructure. In 2025, Nepal imposed widespread social media bans[137] during a period of political unrest, a move that triggered significant public mobilization and youth-led digital activism. Nepal's experience became a regional reference point, illustrating how restrictive digital measures can produce unintended political consequences and intensify demands for digital rights protections.
- These developments resonate strongly with Pakistan's own experience during the February 2024 general elections[138] and Indo Pak escalation[139], when internet slowdowns and platform restrictions were widely reported. The parallel between Nepal and Pakistan demonstrates how internet shutdowns and digital restrictions can diffuse regionally, particularly in politically sensitive contexts, reinforcing a pattern of regulatory borrowing across neighboring states facing similar governance challenges.

[137] https://www.nytimes.com/2025/09/07/world/asia/nepal-bans-social-media-platforms.html

[138] https://www.aljazeera.com/news/2024/2/8/inherently-undemocratic-pakistan-suspends-mobile-services-on-voting-day

[139] https://ooni.org/post/2025-media-censorship-in-india-and-pakistan/

2. Digital communications

- **Which risks do internet shutdowns, network interferences, geo-blocking or other forms of restrictions of connectivity and communications pose to HRDs' work and safety?**

Internet shutdowns and throttling, network interferences, geo-blocking, and other connectivity restrictions are often used as a tool of government repression[140]. These impede the work of human rights defenders and journalists working in these regions, making it difficult to report on human rights violations. Especially during times of elections or natural disasters, such restrictions impede HRDs' ability to provide essential and credible information and resources in real time. Restrictions on connectivity and communications also pose a particular threat to the safety of HRD lives; reliable internet connectivity serves an important purpose in signalling the continued safety of HRDs and journalists, a fact which became most popular through Gazan journalist Bissan Owda's infamous "It's Bissan from Gaza and I'm still alive" opener to each of her videos on her social platforms during the Israel-Palestine conflict.

In countries like Pakistan, internet shutdowns extend to restrictions on mobile network connectivity[141] as most of the population accesses the internet on their mobile phones. With a government moving fast towards a 'Digital Pakistan' - digitising essential services such as banking, health, education, and social security - these restrictions of connectivity and communications leave HRDs especially in rural and farflung areas of Pakistan unable to provide information and services to their communities.

- **What forms of technology-facilitated attacks do HRDs face on social media platforms and digital communications services? How do these online attacks intersect with offline events?**

HRDs are increasingly becoming targets of technology-facilitated threats, which are not just limited to cybersecurity attacks by bad actors, but also include state surveillance. Social media algorithms themselves tend to reward bad behaviour as targeted hate campaigns against HRDs are able to gain a strong footing and in some instances even virality, on these platforms. Hate speech, incitement to violence, hacking, doxxing, bullying, and coordinated smear campaigns are some of the most common threats that HRDs face online.

On the other hand, it has also been widely documented that HRDs end up becoming targets of state surveillance and state-based actors, especially those HRDs working in countries that have

---

140 https://akademie.dw.com/en/out-of-the-dark-new-study-on-internet-shutdowns-in-south-and-southeast-asia/a-73069489

141 https://www.hrw.org/news/2024/12/12/dangerous-digital-crackdown

authoritarian governments. For instance, China's[142] internet is tightly controlled and built for state surveillance, leaving activists under constant monitoring and with limited access to tools like VPNs. Surveillance especially is often normalised[143] and presented as a necessity, often used under the vague umbrella term of 'national security'.

These online attacks intersect with real offline violence, which places not only the work, but the very lives of HRDs, in danger. Front Line Defenders recorded the killings[144] of at least 324 human rights defenders across 32 countries in 2024 alone, in efforts to silence their work and advocacy. Such targeted campaigns and state surveillance combined aim to create a 'chilling effect' in the operational atmosphere of social work within these countries and regions, undermining civic space and freedom of expression by making it unsafe both online and offline.

- **What specific risks to HRDs emerge via online platforms and communications services in situations of armed conflict, instability and/or elections?**

Elections often act as a catalyst for online harm, as political parties tend to exacerbate social tensions for the purposes of electoral gain. According to research[145], in India, anti-Muslim hate speech incidents increased in the midst upcoming elections in 2023.

Internet shutdowns are another trend often witnessed in Pakistan in the run up to elections. Amnesty International has repeatedly reported[146] on this distrubing trend, calling it "a reckless attack on people's rights". These restrictions impede the ability of HRDs to provide essential information to their communities regarding electoral ballots and polling stations.

Online platforms during elections and situations of armed conflict become battlegrounds for TFGBV, disinformation, and mob mobilisation. DRF's report, "Platforms at the Polls[147]", noted: "in the run up to, and even during, the elections included significantly high levels of harmful and hateful content, in clear violation of the community guidelines established by the platforms themselves". DRF's report on TFGBV[148] during the Indo-Pak conflict of May 2025 revealed that social media platforms are used to conduct digital warfare to fuel hostilities and amplify online attacks, which disproportionately target figures in the public eye, such as HRDs and journalists.

---

142 https://freedomhouse.org/country/china/freedom-net/2024
143 https://www.frontlinedefenders.org/es/node/2320
144 https://globaltfokus.dk/images/DDI/Breaking-Points.pdf
145 https://www.aljazeera.com/news/2023/9/26/anti-muslim-hate-speech-in-india-spikes-around-elections-report-says
146 https://www.amnesty.org/en/latest/news/2024/02/pakistan-election-day-internet-shutdown-is-a-reckless-attack-on-peoples-rights/
147 https://digitalrightsfoundation.pk/wp-content/uploads/2024/12/Platforms-at-the-Polls.pdf
148 https://digitalrightsfoundation.pk/wp-content/uploads/2025/05/Digital-Battlegrounds-Report.pdf

- **What specific risks do women HRDs and HRDs from groups affected by marginalisation and discrimination face on online platforms and communications services?**

Women Human Rights Defenders and those from marginalised groups face a distinct spectrum of digital threats that often transition into physical violence, particularly when their work challenges deeply rooted patriarchal or religious structures.

HRDs and journalists face greater abuse in general, especially those with intersecting identities. Both AI-driven algorithms and human actors target them to further endanger their already vulnerable status. Reporting[149] by Musawah on the digital harms faced by Muslim women HRDs in the Greater Horn of Africa sheds further light on this claim. Research[150] by Digital Rights Foundation (DRF) shows that HRDs also part of ethnic or religious minorities or who have a lower socioeconomic or disability status, experience a higher risk of experiencing harmful content.

These issues are exacerbated by the fact that in many regions and in countries like Pakistan, many women and marginalised HRDs lack digital literacy which leaves them particularly vulnerable to online attacks and hacking attempts. This points to the need for providing increased ICT training to these HRDs, as they struggle to navigate an environment that is already hostile towards them.

- **How do companies' policies and practices relating to content moderation and engagement with law enforcement and government authorities affect HRDs' work and safety?**

Companies' content moderation practices and their engagement with government authorities can significantly influence the ability of HRDs to operate safely online. In Pakistan, the interaction between social media platforms and state authorities often under broad legal frameworks regulating online content has created several challenges for HRDs.

- Online platforms often respond to requests from law enforcement agencies such as the National Cyber Crime Investigation Agency (NCCIA)[151] from Pakistan, for data access, account restrictions, or content removal. When companies comply with such requests without strong transparency, independent oversight, or due-process safeguards, HRDs

149 https://www.musawah.org/wp-content/uploads/2022/05/InVisible-The-Digital-Threats-Muslim-Women-Human-Rights-Defenders-Face-in-the-Greater-Horn-of-Africa.pdf

150 https://digitalrightsfoundation.pk/wp-content/uploads/2024/05/White-Paper-A-Southern-and-Southeast-Asian-lens-on-Online-Harms.pdf

151 https://www.nccia.gov.pk/

may face risks including surveillance, identification of anonymous sources, and legal harassment.

- For example, an Islamabad court reportedly ordered the blocking of 27 YouTube channels[152] following a request linked to NCCIA, alleging that the channels were spreading misleading information about state institutions. Several of the affected channels were reportedly run by journalists and commentators. Such actions illustrate how content moderation decisions influenced by government requests can restrict freedom of expression and limit the ability of HRDs to report, document human rights concerns, and engage in public advocacy.
- The combination of restrictive legal frameworks, government monitoring of online spaces, and companies' compliance with state requests creates a chilling effect on HRDs. Activists, journalists, and digital rights defenders may self-censor or avoid addressing sensitive topics due to fear of surveillance, account suspension, legal action, or online harassment. The history of internet shutdowns, particularly during the 2024 general elections of Pakistan, further exemplifies how dissenting voices can be curbed and freedom of expression restricted. Such measures limit the ability of HRDs to communicate, document human rights violations, and engage with both domestic and international audiences.

- **How do advances in AI technologies exacerbate risks to HRDs' operations and presence on online platforms and communications services?**

Advances in AI technologies significantly exacerbate risks to Human Rights Defenders (HRDs) by weaponising data and automating repression. AI-powered surveillance[153], such as facial recognition and biometric profiling, eliminates anonymity in public spaces, allowing hostile actors to track movements and identify activists during protests. Furthermore, highly invasive AI-driven spyware, including 'zero-click'[154] tools like Pegasus, grants attackers total access to encrypted communications without user interaction, effectively dismantling digital safe havens.

---

152 https://digitalrightsmonitor.pk/islamabad-court-approves-fia-request-to-block-27-youtube-channels-under-peca/

153 https://www.gchumanrights.org/preparedness/cyber-protection-for-human-rights-activists-in-key-international-instruments/

154 https://www.hrw.org/news/2022/01/26/human-rights-watch-among-pegasus-spyware-targets

Online platforms further compromise safety through biased algorithmic moderation. AI often suppresses legitimate human rights advocacy while simultaneously failing to recognise nuanced, 'veiled' threats[155] that incite real-world violence. The engagement-driven business models[156] of Big Tech prioritise sensationalism, leading to the algorithmic amplification of smear campaigns, doxxing, and hate speech against HRDs. This creates a tricky situation where activists must rely on surveillance-based platforms to document abuses, inadvertently feeding the data systems[157] used to target them. Ultimately, these technological shifts create a chilling effect, where the fear of automated detection and subsequent physical or legal retaliation via state mechanisms silences dissent and undermines the capacity of HRDs to operate securely.

3. Digital restrictions to privacy

- **What risks have emerged for HRDs with the increasing procurement, use and abuse of digital surveillance tools, including spyware and interception technologies, by State and non-State actors?**

In the context of Pakistan, increased procurement and misuse of digital surveillance capabilities have created significant risks for HRDS as well as journalists and lawyers. These risks include invasive processes such as unlawful monitoring, covert access to personal devices as well as illegal interception. Recent investigations from newspapers in the country such as Dawn[158] and international organizations such as Amnesty International[159] show how state agencies have expanded their surveillance capabilities through systems such as the Lawful Intercept Management System (LIMS), which can monitor mobile phones and communications simultaneously with the help of telecommunications providers in the country. Another development has been the government's use of a Web Monitoring System (WMS), tasked with being able to monitor internet activity and screen the web for content including posts, videos or comments that can be interpreted as anti-state.

Targeted surveillance and hacking campaigns that try to steal personal information and use it against vulnerable groups in an attempt to stifle dissent and opposition further intensify risks to HRDs. For example, in 2018, Amnesty International documented how the state was using

---

[155] https://www.openglobalrights.org/online-threats-real-world-harms-protecting-human-rights-defenders/
[156] https://www.amnesty.org/en/what-we-do/technology/
[157] https://www.americanbar.org/advocacy/global-programs/news/2024/importance-digital-privacy-emerging-technology/
[158] https://www.dawn.com/news/1940726
[159] https://www.amnesty.org/en/latest/news/2025/09/pakistan-mass-surveillance-and-censorship-machine-is-fueled-by-chinese-european-emirati-and-north-american-companies/

sophisticated phishing attacks against a Pakistani activist.[160] And in the present day, the Pakistani government has been found to have deployed the Intellexa "Predator" software to target human rights lawyers in Balochistan. These cases show how the use of commercial spyware tools are increasingly being procured and used to infiltrate activists' devices.

These practices expose HRDS to data theft, harassment, imprisonment and more concerningly, persecution. The recent arrest of human rights lawyers Imaan Mazari and Hadi Chatta is a case in point of how digital surveillance in Pakistan undermines privacy and freedom of expression and also directly threatens the safety and effectiveness of human rights defenders.[161]

- **What risks have emerged for HRDs with the expansion of biometric surveillance infrastructure and increased monitoring of public and digital spaces?**

Large-scale biometric databases maintained by the National Database and Registration Authority (NADRA) collect fingerprints, facial images, and iris scans and are linked to national identity records used for SIM registration, banking, taxes and other vital public services.[162] Given the vast web of personal data linking citizens to all essential government services, the fact that Pakistan still lacks a comprehensive and exhaustive Data Protection Bill[163] raises multiple concerns. State and non-state actors with the proper mechanisms in place can potentially track an individual's movements, communications, and identifies across different systems, increasing the risk of profiling and monitoring.

This is increasingly worrisome knowing that Pakistan's NADRA and FBR systems have been the victim of various hacking incidents and attempts across the past 10 years that have stolen data from over 2 million citizens.[164]

The expansion of Pakistan's Safe City Project has intensified risks over the years and added an additional layer of surveillance for HRDs as well as citizens. Cities such as Lahore, Islamabad, Karachi and Peshawar (amongst many others in the pipeline) have deployed a network of CCTV cameras fitted with facial recognition capabilities which can identify individuals in public

---

160 https://www.amnesty.org/en/latest/news/2018/05/pakistan-campaign-of-hacking-spyware-and-surveillance-targets-human-rights-defenders

161 https://www.amnesty.org/en/latest/news/2026/01/pakistan-authorities-must-end-judicial-harassment-of-lawyers-imaan-mazari-and-hadi-chatta/

162 https://privacyinternational.org/state-privacy/1008/state-privacy-pakistan

163 https://voicepk.net/2025/05/absence-of-data-protection-law-in-the-digital-age-increases-vulnerability/

164 https://tribune.com.pk/story/2509411/nadra-data-leak-1, https://www.brecorder.com/news/40403243/citizens-personal-data-on-dark-web-nadra-asked-to-further-strengthen-cybersecurity-measures, https://www.dawn.com/news/1968167

spaces. With the project being accused of using Israeli-made software in the past[165] and it being the victim of its own major leaks[166] This infrastructure reduces anonymity during political and religious gatherings or protests, enabling authorities (or hackers) to track people and potentially subject them to illegal surveillance.[167]

Without safeguards or avenues for redress within the judicial system, HRDs face the heightened risk of misidentification, profiling, targeting, and the exposure of their sensitive data either about themselves or the communities they represent.

- **How have technological and regulatory developments relating to encryption eased or exacerbated risks to HRDs?**

Regulatory developments in Pakistan have increasingly sought to restrict and contain online activity that puts HRDs at risk. The Prevention of Electronic Crimes Act (PECA), for example, grants authorities broad powers to demand user data, remove online content, and block digital platforms. It also allows law enforcement to arrest, detain and charge people against claims of unlawful content – the definition of which is kept as vague as possible and can include anything deemed “anti-state” by government authorities. Such frameworks create pressure on technology companies and telecommunications providers to enable access to data and compliance with surveillance requests that undermine digital communication.

In addition, the expansion of monitoring systems and internal control mechanism from third party vendors such as the WMS from China, spyware software such as Predator from Intellexa have raised concerns that authorities may attempt to circumvent encryption through device-level surveillance, using phishing or 1-click attacks, and platform regulation. This increases the likelihood that HRDs’ communications via unsecure platforms such as WhatsApp can be exposed through legal orders, hacking attempts or legally bound service providers.

Technological advancements such as the use of AI in facial recognition software and the development of zero-click surveillance attacks (such as Pegasus), further exacerbates existing risks. The ability of technologies and cybersecurity firms to keep adapting to changing landscapes and finding new ways of tapping into personal data means that HRDs are constantly exposed to surveillance and harassment with little to no legal redressal available.

- **How do advances in AI technologies exacerbate risks to the privacy and safety of HRDs?**

---

165 https://profit.pakistantoday.com.pk/2026/03/04/officials-claim-islamabad-safe-city-cameras-are-not-using-israeli-software-any-longer/

166 https://www.dawn.com/news/1459963

167 https://digitalrightsfoundation.pk/august-2018-a-study-on-the-punjab-safe-cities-authority-psca/

The use of AI technologies in the present day whether by state entities in official mechanisms or by Big Tech platforms for profit has opened up new vulnerabilities for individuals especially those in highly risky professions such as HRDs. AI-driven technologies such as facial recognition, data collection, data analytics and image generation enable faster and more accurate surveillance, targeted harassment, and manipulation of information for personal gain.

AI-based facial recognition software when combined with national databases such as NADRA in Pakistan or law enforcement processes (such as the Safe City Project), can facilitate profiling and tracking of HRDs increasing the risk of intimidation. It also increases the risk of bias and discrimination against minority groups, as noted by multiple used cases in the west.[168]

AI also intensifies disinformation and the distortion of facts to exploit people either in the face of conflict or important political events. Deepfake and generative AI technologies, which are largely made accessible to the general public via social media platforms such as X and Facebook, can be used to create fabricated videos or audio clips of HRDs. Various cases have been seen in Pakistan where manipulated political online content has been circulated and gone viral,[169] demonstrating how AI can be used to orchestra smear campaigns, and more often than not, cause online abuse in the form of TFGBV.

In a context of little to no data protection laws, weak judiciary in the face of the state, and limited oversight, these AI-enabled capabilities heighten the risks of unlawful surveillance, gendered harms, and significantly constrain the operational space and safety of HRDs in Pakistan.

4. Corporate responses

- **How are companies meeting their responsibilities to identify, assess, mitigate and respond to risks posed to HRDs on their platforms and services?**

Human rights defenders (HRDs) in Pakistan operate in a digitally restrictive environment where surveillance, censorship, and online harassment routinely intersect. Pakistan's internet governance model combines with expanding legal enforcement under cybercrime and "misinformation" frameworks, recurring platform restrictions (including prolonged disruption/blocks affecting political discourse), and growing technical capacity to filter, slow, or block traffic and VPNs.[170] In practice, this produces "high-risk moments" (elections, protests, securitized events) where HRDs, journalists, political activists, minority rights advocates, and

---

168 https://www.theguardian.com/technology/2025/dec/05/home-office-facial-recognition-tech-issue-black-asian-subjects
https://moderndiplomacy.eu/2025/07/01/chinas-new-facial-recognition-regulations-positive-impacts-and-challenges/

169 https://www.dawn.com/authors/10862/fact-check-by-iverify
https://digitalrightsmonitor.pk/in-south-asia-deepfakes-are-increasingly-used-to-inflict-gendered-harm/

170 https://apnews.com/article/pakistan-cyber-law-social-media-6de3a878c434abb154b91012bc9ca33c

women human rights defenders need fast, predictable platform action, but often face slow escalation paths, limited transparency, and uneven enforcement.[171]

Pakistan-specific data points highlights both scale and urgency. Pakistan's government has made large volumes of content-removal demands to big platforms (e.g., thousands of requests to Google over multi-year periods) and Meta has restricted access to thousands of items in Pakistan under local-law reporting pathways.[172] Meanwhile, civil society service data indicates sustained levels of technology-facilitated abuse with Digital Rights Foundation's own reports recording 3,171 complaints of tech-facilitated gender-based violence in 2024 alone, illustrating the volume of safety incidents that require effective platform reporting, response, and remedy systems.[173]

Under the UN Guiding Principles on Business and Human Rights (UNGPs), companies are expected to identify and assess adverse human rights impacts, prevent/mitigate harms linked to their products or services, and enable remedy where they cause or contribute to harm.[174] In Pakistan, major tech companies show partial alignment through human rights policy commitments, selective "high-risk" operational programs during elections/crises, and transparency reporting and legal request handling, though these mechanisms often prioritize compliance workflows over HRD-centered safety outcomes.

Meta's Corporate Human Rights Policy explicitly frames HRDs as a "high-risk user group," identifies risks including digital security attacks, surveillance, and censorship demands, and states an intent to proactively engage HRDs.[175] In Pakistan, Meta has publicly described deploying an election operations team with expertise spanning election integrity, human rights, safety, and cyber, including local-language capacity, plus "Trusted Partner" channels for reporting harmful content during election periods.[176] Meta's internal escalation systems also function as a backstop when ordinary user-reporting fails in high-risk contexts, this was seen in the Oversight Board case where Meta's High Risk Early Review Operations (HERO) system escalated a blasphemy-accusation post during Pakistan's 2024 election run-up; policy experts removed it based on imminent-harm risk tied to "outing" an alleged blasphemer in Pakistan.[177]

---

171 https://www.reuters.com/world/asia-pacific/pakistani-journalists-rally-against-law-regulating-social-media-2025-01-28/

172 https://www.iradapk.org/wp-content/uploads/2024/01/State-of-indie-Journalism-report-2023.pdf

173 https://digitalrightsfoundation.pk/digital-security-helpline-annual-report-2024/

174 https://www.ohchr.org/sites/default/files/Documents/Issues/Business/Intro_Guiding_PrinciplesBusinessHR.pdf

175 https://humanrights.fb.com/policy/

176 https://www.geo.tv/latest/511973-meta-issues-guidelines-to-protect-election-integrity-in-pakistan

177 https://www.oversightboard.com/decision/ig-wxhs8uei/

In another Oversight Board decisions tied to Pakistan Meta reversed its removal of a Karachi mayoral election comment posted by a journalist that neutrally referenced a designated organization, reflecting how automated or rigid enforcement can wrongly penalize reporting and political discourse.[178] Moreover, in another case the Board upheld leaving up a Pakistani news outlet's post sharing a parliamentary speech under an "awareness raising" exception, reinforcing that HRD and journalistic content can be chilled when platforms fail to consistently apply context-sensitive exceptions.[179]

Additionally, Google's approach is often expressed through transparency about legal process and publishing reporting structures for government requests.[180] Pakistan's environment demonstrates how "local law obligations" can become a censorship vector which was particularly seen in 2025 when YouTube warned more than two dozen Pakistani government critics that their channels could be blocked in Pakistan following a court order alleging "anti-state" content, an example of how platforms may operationalize domestic legal demands even where due process and human rights safeguards are contested.[181]

TikTok operates large-scale content enforcement in Pakistan and also processes significant government removal requests. Pakistan ranked among the highest sources of government removal demands in TikTok's reporting for July-December 2023, with a high proportion of requested content actioned.[182]This is a double-edged pattern for HRDs since it may help remove clearly harmful content, but can also enable overbroad censorship when "morality," blasphemy, or political offense is used to target dissenting voices.[183]

Similarly, court filings reported in Pakistan that X rejected many government content-removal requests on the grounds that content did not violate platform rules, often asking for additional information.[184] At the same time, Pakistan's interior ministry characterized X as failing to comply with government directives and cited this as justification for blocking the platform on national security grounds.[185] For HRDs, this pairing of platform resistance plus state blocking often yields a practical outcome of reduced reach, VPN dependence, and higher digital risk during crises.

---

[178] https://www.oversightboard.com/decision/fb-7uk5f6vg/

[179] https://www.oversightboard.com/news/oversight-board-upholds-metas-decision-in-reporting-on-pakistani-parliament-speech-case/

[180] https://support.google.com/transparencyreport/answer/9713961

[181] https://www.reuters.com/sustainability/society-equity/more-than-two-dozen-critics-pakistan-government-face-youtube-ban-2025-07-09/

[182] https://www.dawn.com/news/1857893

[183] https://www.dawn.com/news/1869462/13m-urls-blocked-over-illegal-content-reveals-telecom-regulator

[184] https://www.dawn.com/news/1863985/

[185] https://www.reuters.com/world/asia-pacific/pakistan-blocked-social-media-platform-x-over-national-security-ministry-says-2024-04-17/

Additionally, in Pakistan, HRD risk is also shaped by private companies supplying filtering and lawful-intercept capabilities. Amnesty International documented how Pakistan's censorship and surveillance capacity (including WMS 2.0 and LIMS) is enabled by a cross-border supply chain involving multiple foreign companies; the report frames this as a "profitable economy of oppression" and links these capabilities to repression of journalists and civil society.[186] This expands the corporate responsibility question from "content moderation" to full-stack digital rights due diligence, covering vendors, telecom enforcement nodes, and platform intermediaries.

- **Are existing corporate models and approaches to risk assessment, due diligence, remedial mechanisms and engagement with HRDs on protection concerns and reports of violations sufficient and/or effective?**

Evidence suggests current models are not sufficient in Pakistan, largely because they are unevenly resourced, event-driven, and skewed toward legal compliance rather than protection outcomes, especially for non-elite or non-English-speaking users. DRF's research highlights a recurring "policy-practice gap" where platforms present extensive public rules on election integrity and harmful content, yet enforcement in Pakistan has remained inconsistent compared with typical Global North readiness.[187] DRF's analysis of Pakistan's 2024 election information ecosystem found persistent gendered disinformation and harmful content, including deepfakes and threats targeting journalists and marginalized groups, suggesting that detection, escalation, and timely enforcement did not match the severity and scale of harms.

Remedial and escalation mechanisms also show structural weaknesses. Internews' assessment of Meta's "Trusted Partner" channel found that partners sometimes wait weeks or months for responses, even for imminent-harm cases, and that the program appeared under-resourced relative to reporting volume problems that carry acute consequences in high-risk countries where civil society often functions as a frontline safety actor.[188] Additionally, Pakistan's high volume of government requests for content restriction and user data, alongside platform compliance rates in some reporting periods, indicates that corporate due diligence must more rigorously assess whether state demands are lawful, necessary, and proportionate, and whether compliance creates predictable pathways for reprisals against HRDs.

- **What challenges do civil society and companies face in ensuring corporate policies, processes and initiatives – including in relation to internal mechanisms**

---

186 https://www.amnesty.org/en/latest/news/2025/09/pakistan-mass-surveillance-and-censorship-machine-is-fueled-by-chinese-european-emirati-and-north-american-companies/

187 https://digitalrightsfoundation.pk/wp-content/uploads/2024/12/Platforms-at-the-Polls.pdf

188 https://internews.org/resource/safety-at-stake-how-to-save-metas-trusted-partner-program

and external engagement – adequately and effectively address the range and extent of risks faced by HRDs in the digital age?

One of the biggest challenges civil society and companies face in Pakistan is the gap between the scale and speed of harm and the slow, inconsistent response mechanisms available on platforms. DRF's reporting shows that online abuse is not episodic but systemic with its Digital Security Helpline recording 3,171 complaints of tech-facilitated gender-based violence in 2024 alone, including cases of doxxing, non-consensual intimate imagery, blackmail, and coordinated abuse, with women disproportionately affected. DRF has also repeatedly warned that certain professions and communities face repeated coordinated hate campaigns but often lack institutional protection, which means civil society groups are forced to act as frontline responders, documenting abuse, supporting survivors, and escalating cases that platforms should be addressing more effectively themselves. This burden becomes even heavier in politically charged periods, when journalists, women in public life, and dissenting voices are targeted at scale, while platform reporting and escalation systems remain opaque, under-resourced, or too slow to prevent harm.

Companies also face a difficult operating environment in Pakistan because state pressure, restrictive regulation, and security narratives often blur the line between legitimate safety enforcement and censorship. News reporting in 2025 showed strong pushback from journalist bodies and rights advocates against expanded social media regulation under PECA amendments, warning that such measures could be used to intimidate journalists and suppress lawful expression.[189] At the same time, civil society has to respond to fast-evolving harms that go beyond content moderation alone, including account compromise and impersonation scams. DRF documented 233 scam-call cases by August 2025 involving WhatsApp account hijacking, and linked these threats to weak reporting systems, poor user awareness, and the absence of stronger data protection safeguards. Many of these accounts belonged to HRDs who became vulnerable to these scams which complicated the already sensitive nature of these cases.

- **What steps should companies take to improve identification, assessment and prevention of risks posed to HRDs' work and safety on their platforms and services?**

Companies should pivot from "policy-forward" to outcome-forward approaches in Pakistan measuring success by reduced harm, faster remedy, and fewer reprisals, rather than by aggregate enforcement volume. This aligns with UNGP expectations to prevent and mitigate adverse impacts and enable remedy, and with emerging platform governance guidance that

189 https://www.reuters.com/world/asia-pacific/pakistani-journalism-body-criticises-new-law-regulating-social-media-2025-01-24/

emphasizes human rights due diligence, transparency, and accountability in platform design and moderation.[190]

Institutionalize Pakistan-specific human rights due diligence (HRDD) and crisis playbooks for elections, protests, and securitized periods, including local-language risk assessment and “rapid harm” escalation relevant to blasphemy accusations, gendered disinformation, and doxxing (rather than relying primarily on virality signals).[191]

Build reliable, audited escalation channels for vetted civil society and newsroom partners with service-level targets (time-to-human-review, time-to-action) and transparent feedback loops, addressing documented delays and operational failures in flagship trusted-partner models.[192]

Increase transparency specific to Pakistan with publishing granular reporting on government requests (content restriction, account actions, and user-data requests), outcomes, and legal bases, so HRDs can assess risk and civil society can verify whether restrictions are proportionate and rights-compatible.[193]

Harden account security and anti-harassment design for high-risk users particularly with stronger default protections, friction against mass harassment, improved recovery for compromised accounts, reflecting the scale of reported abuse and account compromise risks within Pakistan’s ecosystem.[194]

Extend responsibility across the supply chain, including surveillance and filtering vendors by adopting and publishing robust end-use human rights reviews, meaningful export guardrails, and remedy pathways when products enable censorship or unlawful interception, consistent with documented supply-chain links to Pakistan’s surveillance and censorship infrastructure.[195]

---

190 https://www.ohchr.org/sites/default/files/Documents/Issues/Business/Intro_Guiding_PrinciplesBusinessHR.pdf

191 https://www.oversightboard.com/decision/ig-wxhs8uei/

192 https://internews.org/resource/safety-at-stake-how-to-save-metas-trusted-partner-program/

193 https://digitalrightsfoundation.pk/digital-security-helpline-annual-report-2024/

194 https://www.dawn.com/news/1906339

195 https://www.amnesty.org/en/latest/news/2025/09/pakistan-mass-surveillance-and-censorship-machine-is-fueled-by-chinese-european-emirati-and-north-american-companies/