Joint Stakeholder Report
Universal Periodic Review
41st Session - India

Human Rights Online in India

Access Now is an international non-profit organisation which works to defend and extend the digital rights of users at risk globally. Through presence in 13 countries around the world, Access Now provides thought leadership and policy recommendations to the public and private sectors, and also operates a 24/7 digital security helpline.

Website: https://www.accessnow.org/ *Contact Email*: un@accessnow.org

Association for Progressive Communications (APC), an organisation in consultative status with ECOSOC, advocates the strategic use of information and communications technologies to advance human rights. The APC network has 62 organisational members and 29 individual members active in 74 countries, including India.

Contact Address: PO Box 29755, Melville, 2109 - Johannesburg, South Africa
Website: www.apc.org *Contact person:* Veronica Ferrari (veronica@apc.org)

Internet Freedom Foundation ("IFF") is a registered charitable trust which advocates to protect and advance constitutional freedoms in a digital society. IFF works across a wide spectrum of issues, with expertise in free speech, electronic surveillance, data protection, net neutrality and innovation; IFF aims to champion privacy protections, digital security, and individual freedoms in the digital age.

Contact Address: I 1718, Third Floor, Chittaranjan Park, New Delhi - 110019
Website: https://internetfreedom.in/ *Contact Email*: info@internetfreedom.in

I. INTRODUCTION

1. This joint stakeholder report focuses on key issues relating to human rights online in India, including internet shutdowns, digital exclusion, freedom of speech and expression online, online harassment and hate speech, privacy, surveillance and data protection. The report draws on extensive and ongoing monitoring of the situation of human rights online in India by a number of civil society organisations and a desk review.

2. This review marks the fourth cycle for India in the Universal Periodic Review mechanism. During the third cycle, India received nine recommendations relating to free speech, tackling religious discrimination, hate speech and xenophobia against minorities, protection of human rights defenders, privacy and communications surveillance. However, India failed to accept even a single one of these recommendations.[1]

3. Overall, India has accepted only 152 out of 250 recommendations made during the third cycle. In previous cycles, India had accepted 67 out of 169 recommendations (second cycle);[2] and 5 out of 18 recommendations (first cycle)[3].

II. CONTEXT OF THE SITUATION OF HUMAN RIGHTS ONLINE IN INDIA

4. India has been going through an alarming digital authoritarian movement. Over the past few years, the government has taken a series of threatening intimidatory actions against human rights defenders and media personnel, and hastily created regulatory mechanisms that grant them problematic new powers and increased control over content on social media platforms that adversely impact human rights.

5. The Government's efforts to criminalise dissent and censor information include shutting down the internet, preventing journalists from entering protest sites, filing criminal charges against journalists that criticise the Government, and issuing broad advisory directives to social media companies to block critical content. While certain regulatory measures were seemingly created to combat "fake news", restrict illegal content and improve grievance redress mechanisms for users - they create a framework for unnecessary and disproportionate interference with freedom of expression by imposing onerous obligations on intermediaries to take down content, and an oversight mechanism that allows the government to determine what stays online.

---

[1] Human Rights Council, Report of the Working Group on the Universal Periodic Review: India - Addendum, 6 September 2017, https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/36/10/Add.1

[2] Human Rights Council, Report of the Working Group on the Universal Periodic Review: India - Addendum, 17 September 2012, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G12/167/57/PDF/G1216757.pdf?OpenElement

[3] Human Rights Council, Report of the Working Group on the Universal Periodic Review: India – Addendum, 25 August 2008, https://documents-dds-ny.un.org/doc/ UNDOC/GEN/G08/161/58/PDF/G0816158.pdf?OpenElement

6. There have been some positive efforts at the parliamentary level such as the report on the impact of internet shutdowns published by the Standing Committee on Information Technology & Communications.[4] Even though the report falls short of condemning shutdowns altogether given their impact on fundamental rights, the report is significant as the first parliamentary publication documenting the impact of internet shutdowns on fundamental rights and must result in prompt and concrete actions by the Government.

7. The redistribution of power that we are seeing in favour of the Government severely impacts fundamental rights to freedom of speech, expression, online association, and assembly; and this combined with the 2021 Pegasus project revelations (detailed in the Annex below) highlight the pattern of authoritarianism prevalent in India.

III. INTERNET SHUTDOWNS

8. In the year 2020, India imposed the highest number of internet shutdowns in the world.[5] The past five years have seen an unprecedented increase in internet blockades or bandwidth throttling, as a weapon against dissent and protests, to curb freedom of speech and freedom of press, cover up human rights violations and also for administrative convenience. Often, they are imposed in an opaque and disproportionate manner, for reasons such as preventing cheating in exams (as done in Rajasthan and Arunachal Pradesh), and without making the order available in the public domain. This is in contravention of the Indian Supreme Court's judgement in *Anuradha Bhasin v. Union of India*[6], which requires that internet shutdown orders must be lawful, necessary and proportionate, and must also be published to enable those aggrieved to challenge the order before courts. Moreover, such orders can only be issued if it is absolutely necessary to do so. Subsequently, in *Foundation for Media Professionals v. Union of India,* the Supreme Court held that internet shutdown orders must be for a limited period.[7]

9. Despite the aforementioned judgments, internet shutdown orders are far too common. To gauge the scale and severity of the impact of shutdowns, in Arunachal Pradesh the shutdown affected 15 out of the 25 administrative districts of the state.[8] In Rajasthan, the largest state in India, a similar

---

[4] Standing Committee on Communications and Information Technology, Lok Sabha, 26th Report, *Suspension of Telecom Services/Internet and its Impact*, December 2021, http://164.100.47.193/lsscommittee/Communications%20and%20Information%20Technology/17_Communications_and_Information_Technology_26.pdf

[5] Access Now, *#KeepItOn report: India shuts down internet more than any other nation on earth*, Access Now, 3 March 2021, https://www.accessnow.org/keepiton-report-india-shuts-down-internet-more-than-any-other-nation-onearth/

[6] *Anuradha Bhasin v. Union of India (*2020) 3 SCC 637.

[7] 2020 SCC online SC 453

[8] The Telegraph, *Arunachal Internet bar to curb cheating*, 30 October 2020; https://www.telegraphindia.com/north-east/arunachal-internet-bar-to-curb-cheating/cid/1796058,

shutdown affected all administrative districts apart from one.[9] In the **Union Territory of Jammu and Kashmir**, India imposed the longest internet shutdown in a democracy,[10] which has been condemned by UN human rights experts as a form of collective punishment of the people of Jammu and Kashmir, without even a pretext of a precipitating offence".[11] Indian authorities continue to impose repeated shutdowns in Jammu & Kashmir.[12]

10. The Union government of India claims that it does not maintain a record of internet shutdowns implemented at the state level.[13] Trackers maintained by civil society organisations however show a stark reality. The internet shutdowns tracker maintained by SFLC.in has recorded 558 internet shutdowns since the year 2012.[14]

11. In India, the Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017 is the applicable law which regulates imposition of internet shutdowns.[15] Prior to the passage of the 2017 rules, state governments relied on section 144 of the Criminal Procedure Code to impose an internet shutdown.[16]

12. The 2017 Rules have several shortcomings which have also been recognised by the Supreme Court of India. The rules do not provide in clear terms the conditions under which a shutdown can be imposed, which often lead to arbitrary shutdowns being imposed. Further, the rules do not provide an effective review mechanism (the review committee lacks independence as it comprises solely representatives of the executive). The legality of the 2017 Rules is being considered by Gauhati High Court in *Ajit Bhuyan v. State of Assam*.[17]

---

[9] The Indian Express, *Rajasthan shuts Internet as 16 lakh appear for REET 2021*, 27 September 2021,https://indianexpress.com/article/jobs/rajasthan-shuts-down-internet-as-16-lakh-sit-for-teacher-exam-7536304/.

[10] The Washington Post, *India's internet shutdown in Kashmir is now the longest ever in a democracy*, 16 December 2019, https://www.washingtonpost.com/world/asia_pacific/indias-internet-shutdown-in-kashmir-is-now-the-longest-ever-in-a-democracy/2019/12/15/bb0693ea-1dfc-11ea-977a-15a6710ed6da_story.html; Access Now, *#KeepItOn update: who is shutting down the internet in 2021?*, 7 June 2021, https://www.accessnow.org/who-is-shutting-down-the-internet-in-2021/.

[11] Special Procedures, *UN Rights Experts urge India to end communications shutdown in Kashmir*, 22 August 2019, https://www.ohchr.org/en/press-releases/2019/08/un-rights-experts-urge-india-end-communications-shutdown-kashmir?LangID=E&NewsID=24909

[12] Scroll.in, *Internet services across Kashmir suspended on Republic Day*, 26 January 2022, https://scroll.in/latest/1015983/internet-services-across-kashmir-suspended-on-republic-day.

[13] Standing Committee on Information Technology and Communications, *Suspension of Telecom Services/Internet and its Impact*, December 2021, http://164.100.47.193/lsscommittee/Communications%20and%20Information%20Technology/17_Communications_and_Information_Technology_26.pdf.

[14] https://internetshutdowns.in/. The organisation defines an internet shutdown as "*a Government imposed disablement of access to the Internet as a whole within a particular locality or localities for any duration of time*."

[15] Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017 issued under section 7(2)(5) of the Indian Telegraph Act, 1885.

[16] Criminal Procedure Code 1973, Section 144.

[17] PIL No. 79 of 2019

13. These shutdowns not only restrict freedom of speech and expression but also have an immense impact on livelihood, education and health.[18] During the pandemic, such shutdowns, especially the long term shutdown in Kashmir, has resulted in loss of livelihood and education and increased hardships particularly for vulnerable sections of society.

IV. DIGITAL EXCLUSION

14. The use of artificial intelligence-based systems in the country has resulted in both deliberate and unintended exclusions of sections of society from the implementation of these systems, particularly religious minorities and transgender communities.

15. For instance, a Document Segregation and Meta Data Entry (DOCSMEN) software was deployed[19] to digitise legacy data development of 39 million applicants in the National Register of Citizenship (NRC) in Assam, with 1.9 million being excluded from the final list. The inclusion in the NRC list was based on a 'legacy document' which required applicants to show connection to an ancestor who was included in an NRC done in 1951 or in the voter's list of 1966. The legacy data documentation required the presentation of an enormous amount of data, and still the 'family tree' algorithm which was used to verify a person's legacy data excluded several in this process. Mild variations in spelling of names and addresses led to exclusion[20].

16. Further, persons registered in a D-voter list (the doubtful voter's list) in the Assam NRC of 1951 and the 'reference cases' registered by the border police at the time were excluded from the current NRC. In this process, if there were multiple people with the same names and ancestral names and one of them happened to be in the reference case list or the D-voters list, all of them ended up getting excluded. The border police, deployed widely in Muslim dominant districts, has the right to search and collect the fingerprints of any 'doubtful' people.

17. In a similar way, trans-people were excluded from the NRC list. Trans people often have a combination of either missing documents because they fled abusive homes when they were young, or documents that were inconsistent.[21]

---

[18] Digital Empowerment Foundation, Kept in the Dark. Social and Psychological impacts of network shutdowns in India, https://www.apc.org/sites/default/files/Internet-Shutdown-Primer.pdf

[19] Wipro's Page on Citizen Enrolment software, https://www.wipro.com/public-sector/digital-governance--achieving-citizen-enrolment-in-record-time0/#:~:text=Wipro%20partnered%20with%20the%20Government,100%25%20enrolment%20of%20Indian%20citizens.&text=Assam%20has%20been%20grappling%20with%20the%20issue%20of%20undocumented%20immigration%20since%20independence.

[20] Scroll.in, *Bengali Muslims who migrated to Assam in 1871 are not 'illegal Bangladeshis'*, 4 June 2014,https://scroll.in/article/664077/bengali-muslims-who-migrated-to-assam-in-1871-are-not-illegal-bangladeshis ; The Wire, *Assam NRC: A history of violence and persecution*, 15 August 2019, https://thewire.in/rights/assam-nrc-a-history-of-violence-and-persecution

[21] Indian Express, *Delhi: Women and Queer Collectives Say CAA and NRC will hit them Hard*, 4 January 2020, https://indianexpress.com/article/cities/delhi/delhi-women-and-queer-collectives-say-caa-and-nrc-will-hit-them-hard-6198794/

Around 2000 transpeople were excluded as a result of this, and a legal battle is ongoing.[22]

18. Additionally, using AI to look into datasets the Aadhaar is linked to, and enforcing it to avail welfare benefits in a system where access itself is an issue, has led to several exclusions. For instance, the Telangana state government is actively using Samagra Vedika - an integrated platform comprising a 360-degree profile of every citizen in the State; which is being used to know if an applicant is truly eligible for a welfare scheme. However, news reports show that using the Samagra Vedika system, the government initiated mass cancellations of ration cards which enable access to food under the public distribution system.[23] Some cancellations were due to the failure of the card holder to draw ration for six months, though such failure was caused by inability to use the ration card as their fingerprints were not getting detected by the machine.

V. FREEDOM OF SPEECH ONLINE

(i) Criminalisation of Online Speech

19. Legitimate expression on the internet is increasingly being criminalised through application of various laws in India. One of the most widely used laws in recent times for this purpose is the colonial-era offence of sedition under section 124A of the Indian Penal Code, punishable by imprisonment which can extend to life.[24] In 1962, the Indian Supreme Court had laid down guidelines on how Section 124A should be applied, further clarifying that mere dissent will not amount to sedition.[25]

20. Despite this, section 124A has continued to be used, contrary to the guidelines, to stifle legitimate opposition to the government through the years, and more recently, for various expression online. Since 2010, 102 cases have been filed under section 124A against 152 people for creating audios, photos or videos or for sharing content on social media across India, with a majority of the cases filed in the last 4 years.[26] Sedition cases have been filed for a number of reasons, including partaking in a private phone conversation on

---

[22] The Wire, *The NRC Poses a Two-Fold Predicament for Assam's Transgender Community*, 8 October 2019, https://thewire.in/rights/nrc-exclusions-assam-transgender

[23] Caravan, Cancelled ration cards deprived Telangana's poor of food rations amid lockdown, 21 August 2020, https://caravanmagazine.in/government/cancelled-ration-cards-deprived-telanganas-poor-of-food-rations-amid-lockdown

[24] Section 124A, Indian Penal Code, https://indiankanoon.org/doc/1641007/. The offence seeks to charge persons who, "*by words, either spoken or written, or by signs, or by visible representation, or otherwise, brings or attempts to bring into hatred or contempt, or excites or attempts to excite disaffection towards, the Government established by law in India".*

[25] *Kedar Nath Singh v. State Of Bihar,* 1962 AIR 955, https://indiankanoon.org/doc/111867/

[26] Article 14, *Karnataka Has More Sedition Cases Based On Social-Media Posts Than Any State. Most Are Illegal*, 13 July 2021 https://article-14.com/post/karnataka-has-more-sedition-cases-based-on-social-media-posts-than-any-state-most-are-illegal-60ecf64da7945

the situation of the Indian army that was leaked on social media[27], social media posts supporting Pakistan against India in a cricket match[28], criticism of the government's handling of the Covid-19 pandemic[29], sharing a cartoon on India's government and judiciary on Facebook[30], tweeting about the farmers protests[31] and developing of an online 'toolkit' calling for peaceful protest against laws enacted by the government[32].

21. The conviction rate for sedition cases has been extremely low, with under 4% of all cases filed resulting in a conviction[33]; however, in many cases, despite tenuous allegations backed by little evidence, the process has become the punishment for those accused, who have been forced into a long drawn legal process, including incarceration and struggle for bail. In an ongoing petition seeking to strike down Section 124A of the IPC, the Chief Justice of India has noted the misuse of the section by state agencies and the lack of accountability for those responsible[34].

22. Other laws have also been used to criminalise expression online, including sections of the Unlawful Activities (Prevention) Act, 1967 (the 'UAPA')[35]. The UAPA, which was initially implemented to promote and ensure national integration, was later amended in 2004[36] and subsequently 2019[37] to include provisions to counter terrorism and other unlawful activities. The UAPA gives the State the power to designate anyone as a 'terrorist' with little evidence, and detain them for up to 180 days without filing a chargesheet. Concerns have been raised repeatedly on the use of the UAPA to stifle free speech and other civil liberties in the country. For instance, last year, four Supreme Court lawyers and 102 other social media users were charged under the UAPA for social media posts on the violence against minorities in the state of Tripura[38].

---

[27] Indian Express*, Ladakh Cong councillor booked over 'seditious phone conversation',* 20 June 2020 https://indianexpress.com/article/india/ladakh-police-congress-councillor-booked-for-leaked-phone-calls-6467506/
[28] The Wire, *Students Arrested in Agra for 'Supporting Pakistan' During T20 Match May Be Charged With Sedition,* 28 October 2021, https://thewire.in/rights/six-arrested-across-agra-udaipur-and-jammu-for-supporting-pakistan-during-t20-match
[29] The Quint, *Supreme Court Quashes Sedition Case Against Journalist Vinod Dua*, 3 June 2021, www.thequint.com/news/law/supreme-court-quashes-sedition-case-against-journalist-vinod-dua
[30] The Wire, *Bastar Scribe Booked For Sedition For Sharing Loya Case Cartoon on Facebook*, 1 May 2018, https://thewire.in/media/bastar-scribe-booked-for-sedition-for-sharing-loya-case-cartoon-on-facebook
[31] Indian Express, *Sedition FIRs against Tharoor, journalists, now in five states,* 31 January 2021, https://indianexpress.com/article/india/sedition-firs-against-tharoor-journalists-now-in-five-states-7168390/
[32] Article 14, *How the Law was Misused in the Arrest of Disha Ravi,* 16 February 2021, https://www.article-14.com/post/how-the-law-was-misused-in-arrest-of-disha-ravi
[33] Indian Express, *NCRB report: Sedition cases up in 2019 but conviction at all-time low*, 2 October 2020, https://indianexpress.com/article/india/ncrb-report-sedition-cases-up-in-2019-but-conviction-at-all-time-low-6664179/
[34] The Hindu, *Why do you need the 'colonial law' of sedition after 75 years of Independence, CJI asks govt.*, 15 July 2021, https://www.thehindu.com/news/national/is-this-law-necessary-sc-seeks-centres-response-on-pleas-challening-sedition-law/article35336402.ece
[35] https://www.mha.gov.in/sites/default/files/A1967-37.pdf
[36] Unlawful Activities (Prevention) Amendment Bill, 2004, https://prsindia.org/files/bills_acts/acts_parliament/2004/the-unlawful-activities-(prevention)-amendment-act-2004.pdf
[37] Unlawful Activities (Prevention) Amendment Bill, 2019, https://egazette.nic.in/WriteReadData/2019/210355.pdf
[38] Indian Express, *Tripura violence: After SC lawyers, 102 social media accounts face UAPA charge*, 7 November 2021,

Similarly, charges under the UAPA were filed against various persons in Kashmir for “misusing social media”[39]. A petition challenging the constitutional validity of some sections of the UAPA is currently being heard in the Supreme Court of India[40].

23. Section 66A of the Information Technology Act, 2000 (the IT Act), introduced by amendment in 2008, penalized sending "offensive messages" via online communication. The wide powers of the section were frequently used to stifle political dissent. In March 2015, the whole provision of section 66A was declared unconstitutional by the Supreme Court in *Shreya Singhal v. Union Of India* as it violated the right to freedom of expression guaranteed under Article 19(1)(a) of the Constitution of India.[41] However, studies have highlighted the continued use of section 66A, including cases registered after the *Shreya Singhal* decision.[42]

24. In response to a petition filed by civil society organisations, in February 2019, the Supreme Court directed the Union of India to ensure compliance with its decision by making available copies of the judgement to Chief Secretaries across the country, and the sensitisation of police departments.[43] However findings on Zombie Tracker[44] indicated that as many as 810 cases under S.66A are pending before the district courts in 11 States even post 2019. These findings have been used to approach the Supreme Court again, in response to which the Ministry of Home Affairs issued a notification in July 2021 directing all law enforcement authorities to stop registering new cases under Section 66A and to withdraw all pending cases immediately.

(ii) Censorship & Website Blocking

25. Legal Provisions in India, including the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (the **Intermediary Guidelines**), **t**he Cinematograph Act, 1952 (which establishes a Board that has the power to censor movies)[45], and section 95 of the Criminal Procedure

---

https://indianexpress.com/article/north-east-india/tripura/tripura-violence-102-social-media-accounts-booked-under-uapa-7610506/

[39] India Today, Govt slaps UAPA on those 'misusing' social media in Kashmir, Owaisi says new records of cruelty, 18 February 2020, https://www.indiatoday.in/india/story/govt-slaps-uapa-on-those-misusing-social-media-in-kashmir-owaisi-says-new-records-of-cruelty-1647469-2020-02-18

[40] Indian Express, *Supreme Court issues notice to Centre on plea against UAPA*, 18 November 2021, https://indianexpress.com/article/india/supreme-court-issues-notice-to-centre-on-plea-against-uapa-7628000/

[41] *Shreya Singhal v. Union of India AIR 2015 SC 1523*

[42] Abhinav Sekhri & Apar Gupta, *Section 66A and other Legal Zombies*, IFF Working Paper No 2/2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3275893

[43] *People’s Union of Civil Liberties v. Union of India & Othrs,* MA 3220/2018 in W.P. (Crl.) No. 199/2013

[44] A platform built by the Internet Freedom Foundation in collaboration with Civic Data Labs. See https://zombietracker.in/

[45] The Cinematograph Act, 1952, accessed at https://legislative.gov.in/sites/default/files/A1952-37.pdf and the Cinematograph (Certification) Rules, 1983, accessed at https://legislative.gov.in/sites/default/files/A1952-37.pdf. A list of art censorship can be accessed at https://sflc.in/timeline-art-censorships.

Code (under which authorities can ban books)[46] legalize the broad censorship of content by the Indian government, including on the internet.

26. The Intermediary Guidelines, which were brought in by way of an executive order issued in February, 2021 give the Indian government new powers to force social media intermediaries, digital news platforms and OTT platforms to comply with demands of censorship by the government. These rules promote self-censorship and stifle freedom of expression online.[47] The government can also block access to online content if these Guidelines are violated. United Nations independent experts have issued a joint statement highlighting various provisions in the Guidelines which fail to meet the requirements of international human rights laws and standards related to the rights of privacy and freedom of speech and expression.[48] The validity of the Guidelines has been challenged before various High Courts in the country.

27. The Intermediary Guidelines establish two layered self-regulation mechanisms and an oversight body (an executive body); the multiple obligations created for online intermediaries will result in over regulation of the digital space. Additionally, they mandate 'significant social media intermediaries' to provide for traceability of sender of messages which will require the service provider to create a backdoor in end to end encryption. Such a backdoor will result in breach of privacy and impact freedom of speech of users.

28. The Intermediary Guidelines also cover regulation of content of the digital news platforms, despite the parent statute under which the Guidelines were issued (the IT Act) not covering digital press within its scope. Further, the Central Government has introduced new Central Media Accreditation Guidelines, 2022.[49] These guidelines, specifically clause 6.8 (which allows suspension or withdrawal of a journalist's accreditation on a number of broad and vague grounds), restrict the freedom of press and cause a chilling effect on free speech.

29. Additionally, legal provisions such as Sections 69A and 79 of the IT Act, allow the Central Government and the various courts in the country to issue website-blocking orders that Internet Service Providers (ISP) are legally bound to comply with. Blocking directions issued are required to follow the due process as envisaged in the Information Technology (Procedure and

---

[46] A timeline of bookbans can be accessed at https://sflc.in/read-me-not-list-banned-books-india and https://sflc.in/timelineofbookbans.
[47] https://time.com/5946092/india-internet-rules-impact/
[48] Special Rapporteur on Freedom of Expression and Opinion, Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association and the Special Rapporteur on the Right to Privacy, *Comments on the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021* – IND 8/2021, https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=26385
[49] The Central Media Accreditation Guidelines, 2022, https://static.pib.gov.in/WriteReadData/userfiles/file/CentralMediaAccreditationGuidelines2022.pdf.PDFNA9X.PDF

Safeguards for Blocking for Access of Information by Public) Rules, 2009.[50] However, the 'confidentiality' clause continued in these rules as well the broad grounds of 'national security' have been used by the Government to deny right to information requests which seek to make public the website blocking directions issued by the government. For example, information relating to the recent apps block incident was denied to SFLC.in and other civil society organizations.

30. The blocking of websites, social media accounts and applications is also on a rise. The information provided by the Ministry of Electronics and Information Technology to the Parliament shows a steady increase in the number of URLs blocked in recent years, from 471 URLs in 2014; to 9849 in 2020 and 6096 in 2021.[51]

VI. ONLINE HARASSMENT AND HATE SPEECH

(i) ***Hate Speech, Threats and Incitement towards Religious Minorities***

31. Over the past few years, there has been a steady rise in hate and communal violence against persons belonging to minority religions in India. This has been propelled by state complicity and rampant hate speech[52] in media, offline and online spaces, including by influential political actors, which is then amplified on social media and mass media.[53]

32. In 2020, India experienced historic protests against the discriminatory Citizenship Amendment Act[54] and the National Register of Citizens. In the aftermath of the implementation of the National Register of Citizens in the Indian state of Assam, Facebook[55] and other social media was flooded with hate speech against Muslims, calling them "parasites" and "rats", and calling for them to be exterminated. Similar hate speech was propogated on online platforms against protestors, especially those belonging to the Muslim community, campaigning against the Citizenship Amendment Act[56], and

---

[50] Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009https://www.meity.gov.in/writereaddata/files/Information%20Technology%20%28%20Procedure%20and%20safeguards%20for%20blocking%20for%20access%20of%20information%20by%20public%29%20Rules%2C%202009.pdf

[51] Government of India, Ministry of Electronics and Information Technology, Lok Sabha, *Banning Social Media Handles,* 2/2/2022, http://164.100.24.220/loksabhaquestions/annex/178/AU30.pdf. Government of India, Ministry of Electronics and Information Technology, Lok Sabha, *Social Media Intermediaries,* 15/12/2021 http://164.100.24.220/loksabhaquestions/annex/177/AU2813.pdf

[52] *APC at the Human Rights Council 43rd session: Briefing on the deteriorating human rights situation in India*, 4 March 2020, https://www.apc.org/en/pubs/apc-human-rights-council-43rd-session-briefing-deteriorating-human-rights-situation-india

[53] https://www.newindianexpress.com/nation/2019/apr/12/shah-infiltrators-are-termites-bjp-will-weed-them-out-1963206.html; https://www.youtube.com/watch?v=XuNn7JoH4hg

[54] https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25425&LangID=E

[55] https://time.com/5712366/facebook-hate-speech-violence/

[56] https://thewire.in/tech/facebook-saw-spikes-in-hate-speech-in-india-after-caa-protests-and-covid-19-lockdown

against Sikh protestors during the farmers' protests, with many of them being labelled "khalistani" and "terrorists"[57].

33. The situation for religious minorities also worsened with a steep rise in Islamophobic and other hate speech, and misinformation against the backdrop of the COVID-19 pandemic, where political leaders[58] took to social media to propagate misinformation and stigma against minorities[59]. Terms like "Corona Jihad" and "Tablighi Virus" were repeatedly used across mainstream and social media to dehumanise and blame minorities for the spread of the virus, resulting in threats to their life and social boycott[60].

34. Further, despite social media platforms like Facebook and WhatsApp being key mediums through which such hate speech has been perpetuated, little has been done by the platforms to curb the problem. In fact, reports from the *Wall Street Journal* (WSJ)[61] revealed that Facebook India's top policy executive was involved in opposing and preventing the application of the platform's hate speech rules to members of the governing party in India.

35. Hate speech has the effect of routinising discrimination and even physical violence, ultimately paving the way for communal disharmony and genocide. It is clear that the hate speech and incitement to violence propagated during the CAA and NRC protests laid the groundwork for the violence carried out subsequently against Muslim minorities in New Delhi[62].

36. There has also been harassment and threats against minorities through the targeting of women from different communities, particularly by depriving them of their agency to make decisions relating to their religion and faith. Right-wing Hindu groups have perpetuated propaganda using Facebook and WhatsApp around a movement called "Love Jihad", where they claim that there is a concerted effort by Muslim men to convert women from their religion into Islam[63]. More recently, the phone numbers and addresses of Muslim women students, who were protesting their right to wear hijab in educational institutions, were leaked online, resulting in them being doxxed and abused[64].

37. The Preamble of the Constitution of India explicitly recognises the secular nature of the State while Articles 25, 26 and 28 guarantee and limit freedom of

---

[57] https://thewire.in/agriculture/farmers-protest-despite-rightwing-propaganda-khalistani-angle-finds-little-traction;
[58] https://scroll.in/article/959806/covid-19-how-fake-news-and-modi-government-messaging-fuelled-indias-latest-spiral-of-islamophobia
[59] https://www.aljazeera.com/news/2020/04/buy-muslims-bjp-leader-india-calls-boycott-200429034119722.html
[60] Laxmi Murthy, *The Contagion of Hate in India*, https://www.apc.org/sites/default/files/APC_Hate_Speech_V10_0.pdf
[61] https://www.wsj.com/articles/facebook-hate-speech-india-politics-muslim-hindu-modi-zuckerberg-11597423346
[62] https://time.com/5794354/delhi-riots-muslims-india/
[63] India Today, *Over 2500 women converted to Islam in Kerala since 2006, says Oommen Chandy*, 4 September 2012, www.indiatoday.in/india/south/story/love-jihad-oommen-chandy-islam-kerala-muslim-marriage-115150-2012-09-04
[64] https://www.apc.org/en/pubs/hrc-49-oral-statement-online-hate-speech-targeting-religious-minorities

religion and conscience. Sections 153-A 153-B and 505 of the Indian Penal Code (IPC), deal with hate speech, Section 295A penalises those who insult religion or religious freedoms and Section 298 deals with uttering words that may wound religious feelings. Besides these a vast body of provisions are used to address hate speech in India.[65] The Law Commission in India is currently preparing a law on hate speech.[66] However, there has been very little action taken by authorities against those who have engaged in hate speech or incitement to violence against religious minorities. Instead, the broad scope of some of these laws has resulted in curbing legitimate expression of minorities in many instances.

(ii) Technology-facilitated Gender-based Violence, Harassment & Abuse

38. Technology-facilitated gender-based violence (TGBV) includes actions that harm others based on their sexual or gender identity or by enforcing harmful gender norms. These actions are carried out using the internet and/or mobile technology and include stalking, bullying, sex-based harassment, defamation, hate speech, exploitation and gendertrolling.[67]

39. India has a high gender gap in mobile ownership – women are 46% less likely than men to own mobiles.[68] Only 11% of women have internet access. The gender divide in terms of digital access only exacerbates the magnitude of online violence against girls, women and LGBTQIA+ persons who are disproportionately affected by TGBV.[69] A survey shows that 58% girls and young women have faced online harassment/abuse.[70] Over 85% respondents in a study by the International Center for Research on Women who experienced TGBV reported fearing for their own safety; experiencing anxiety or depression; and reducing their online behaviours.[71]

40. According to the National Commission for Women, online harassment cases saw an increase by five times since the COVID outbreak - from 300

---

[65] Center for Communication Governance, *Hate Speech laws in India*, 2018 https://ccgnludelhi.wordpress.com/2018/05/04/launching-our-mapping-report-on-hate-speech-laws-in-india/
[66] The Hindu, *Centre Plans laws on Online Hate Speech,* 19 March 2018, https://www.thehindu.com/news/national/centre-moves-for-law-on-online-abuse/article23295440.ece
[67] International Center for Research on Women, 'Defining and measuring technology-facilitated gender-based violence', 2018, https://www.icrw.org/wp-content/uploads/2019/03/ICRW_TFGBVMarketing_Brief_v4_WebReady.pdf, Association for Progressive Communications, *Online Gender-based Violence*, November 2017, https://www.apc.org/sites/default/files/APCSubmission_UNSR_VAW_GBV_0_0.pdf
[68] LIRNEasia, *AfterAccess: ICT access and use in India and the Global South*, 2018, https://lirneasia.net/wp-content/uploads/2018/08/LIRNEasia-AfterAccess-India-ICT-access-and-use-in-India-and-the-Global-South.pdf
[69] Observer Research Foundation, *Decoding gendered online trolling in India*, 2020, https://www.orfonline.org/expert-speak/decoding-gendered-online-trolling-in-india/
[70] Plan International, *Free to Be Online? A report on girls' and young women's experiences of online harassment*, 2020, https://plan-international.org/publications/freetobeonline
[71] International Center for Research on Women, *Technology-facilitated gender-based violence in the time of COVID-19*, 2020, 'https://www.icrw.org/technology-facilitated-gender-based-violence-in-the-time-of-covid-19/

complaints of online harassment to 1,500 post-COVID.[72] Increased TGBV during COVID has impacted survivors' psychological, social and reproductive health, translated into offline physical and sexual violence, restricted their access to online services, and diminished participation from women with multiple identities due to targeted discrimination and hate speech.[73]

41. Gender trolling, or targeted hate speech against women and gender minorities, has been used in increasing frequency against women journalists and activists who are politically vocal online. This ranges from sexist comments to rape and death threats and even the use of technological applications like *tek fog* to aid in these targeted campaigns.[74] For instance, a study of Twitter mentions of 95 Indian female politicians shows that one-in-five tweets were sexist or misogynistic. Many of those targeted often exit online spaces or restrict their online visibility.[75]

42. Another prominent form of online violence is image-based abuse like non-consensual intimate imagery (NCII), the first conviction for which took place only in 2018.[76] Among the youth, cyberbullying is an increasing concern as India has one of the highest global rates at 53%.[77] Lastly, a form of TGBV that is often unaccounted for are blank calls; 1 in 3 women who use mobiles in India face harassment, receive inappropriate calls.[78]

43. Several reports have also highlighted targeted harassment of Muslim female journalists and activists.[79] In January 2022, hundreds of Muslim women were listed for "auction" on the 'Bulli Bai' app - a clone of 'Sulli Deals' which had also targetted Muslim women less than a year ago.[80] An Amnesty report also

---

[72] Indian Express, *'After Covid, cases of online harassment spiked by 5 times'*, 7 January 2021, https://indianexpress.com/article/cities/ahmedabad/after-covid-cases-of-online-harassment-spiked-by-5-times-7137386/

[73] UN Women,*Online and ICT-facilitated violence against women and girls during COVID-19*, 2020, 'https://www.unwomen.org/sites/default/files/Headquarters/Attachments/Sections/Library/Publications/2020/Brief-Online-and-ICT-facilitated-violence-against-women-and-girls-during-COVID-19-en.pdf

[74] The Wire, T*ek Fog: An App With BJP Footprints for Cyber Troops to Automate Hate, Manipulate Trends*, 6 February 2022, https://thewire.in/tekfog/en/1.html

[75] IT For Change, *Submission on Online Violence Against Women to the Special Rapporteur on Violence Against Women*, 2017, https://itforchange.net/submission-on-online-violence-against-women-to-special-rapporteur-on-violence-against-women

[76] *State of West Bengal v. Animesh Boxi* https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2018/06/State-of-West-Bengal-v.-Animesh-Boxi.pdf

[77] United National Education, Scientific and Cultural Organization,'*From Insult to Inclusion*', 2015, https://unesdoc.unesco.org/ark:/48223/pf0000235414

[78] Economic Times, *Stalker alert: 1 in 3 women who use mobiles in India face harassment, receive inappropriate calls*, 25 March 2019, https://economictimes.indiatimes.com/magazines/panache/stalker-alert-1-in-3-women-who-use-mobiles-in-india-face-harassment-receive-inappropriate-calls/articleshow/68556513.cms

[79] Reporters without Borders, 'Online Harassment of Journalists: Attack of the trolls', 2018, https://rsf.org/sites/default/files/rsf_report_on_online_harassment.pdf

[80] The Print, 'Bulli Bai app conspiracy to persecute minority, promote violence against Muslim women: IWPC', 2022, https://theprint.in/india/bulli-bai-app-conspiracy-to-persecute-minority-promote-violence-against-muslim-women-iwpc/795390/

found that Muslim women politicians received 94.1% more ethnic or religious slurs than women from other religions.[81]

44. While the digital space has been a forum for self-expression, it has also been a platform for queerphobic abuse like the online harassment of a trans-rights activist who started an online fundraiser[82] or the case of a popular YouTuber who used homophobic and casteist slurs in his video.[83]

45. Existing legislation on sexual violence, harassment, criminal intimidation and other forms of online violence are inadequate and often women and gender minorities are hesitant to engage in this lengthy process.[84] While there are some sections in the Indian Penal Code and the IT Act that the police and judiciary use to address the different forms of online abuse, they are often ad hoc or disconnected. Moreover, they are either focused on offline gender-based violence or on online fraud and are not framed within the context of gender and violation of integrity and personal autonomy.

VII. PRIVACY, SURVEILLANCE & DATA PROTECTION

(i) Usage of Mass and Targeted Surveillance, Spyware and Hacking

46. Presently, the Union Government and State Governments are empowered to conduct surveillance under section 5(2) of the Indian Telegraph Act, 1885 ('Telegraph Act')[85] and section 69 of the IT Act[86]. Under rule 419-A of the Telegraph Rules, 1951[87] which governs the process under section 5(2) of the Telegraph Act, the authorised officer is permitted to direct interception of messages only 'on the occurrence of public emergency' or 'if it is in the interest of public safety'. Under section 69 of the IT Act and rules prescribed thereunder,[88] the authorised officer may issue directions for interception if it is in interest of the grounds stated therein which are similar to those listed under Section 5(2) of the Telegraph Act. In addition to these provisions, a "Standard Operating Procedure" was issued by the Ministry of Home Affairs.[89]

---

[81] Amnesty International, 2020. 'Troll Patrol India', https://decoders.blob.core.windows.net/troll-patrol-india-findings/Amnesty_International_India_Troll_Patrol_India_Findings_2020.pdf
[82] The Wire,. 'Trans Rights Activist Misgendered, Trolled After Starting Online Fundraiser', 2021, https://thewire.in/lgbtqia/trans-rights-activist-misgendered-trolled-after-starting-online-fundraiser
[83] Singh, S. K., 'Queerphobia over Social Media in India' Economic & Political Weekly 57: 4, 2022, https://www.epw.in.elibrary.ashoka.edu.in/journal/2022/4/commentary/queerphobia-over-social-media-india.html
[84] The Indian Express, '*Fighting online sexual harassment is a long-drawn battle for women*', 26 January 2022, https://indianexpress.com/article/technology/tech-news-technology/fighting-online-sexual-harassment-is-a-long-drawn-battle-for-women-7741112/
[85] The Indian Telegraph Act 1885
[86] The Information Technology Act 2000
[87] The Indian Telegraph Rules, 1951
[88] The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009
[89] Standard Operating Procedure for interception' (Ministry of Home Affairs, May 19 2011) accessed 24 March 2022

47. However, this surveillance framework suffers from multiple drawbacks. Firstly, the existing surveillance framework does not provide opportunity for either judicial or parliamentary review or oversight and is effectuated entirely by the executive. In the absence of such oversight, this framework is violative of the proportionality standard espoused in the Supreme Court's decision in *K.S. Puttaswamy v. Union of India*[90] as proportionality requires the executive to provide sufficient procedural safeguards. It also violates existing principles of 'separation of powers', by concentrating all surveillance powers with the executive, and 'due process of law', as there is no effective remedy against surveillance, which by its very nature, is carried out in secret.[91] Secondly, with the advancement of technology, targeted surveillance is now being conducted through extremely sophisticated software/hardware, use of which has not been regulated by any existing Indian law. Methods of targeted surveillance have been increasingly used by the Indian government to target journalists, politicians and human rights defenders in India, including through the use of Pegasus spyware. Details of instances of such surveillance are provided in the *Annex* to this report.

48. The existing legal provisions regarding surveillance only relate to targeted interception of calls and messages/data. However, mass surveillance, i.e., indiscriminate surveillance of entire populations or categories of individuals is increasing through government actions in the absence of any legislation to regulate it. Such surveillance is not permissible as it is not prescribed by law. However, massive amounts of personal data is being collected, processed, and shared further by police and security/intelligence agencies that operate in the absence of any legislative basis or effective oversight. These actions violate several rights under the Constitution including the rights to life & liberty, privacy, and freedom of movement. They also have the potential to have a chilling effect on the rights to freedom of speech & expression and peaceful assembly & protest.

49. Details of instances of mass surveillance which are being undertaken in India are detailed in the *Annex*, including the use of the National Automated Facial Recognition System, the National Intelligence Grid (an integrated IT solution which would allow user agencies to access data gathered from various databases) and the Centralised Monitoring System (an ambitious surveillance system that monitors text messages, social-media engagement and phone calls).

(ii) Data Protection

50. In the absence of a data protection law in India, people's data and right to privacy have been vulnerable to continuing exploitation by the private and

[90] *K.S. Puttaswamy v. Union of India* [2017] 10 SCC 1
[91] Apar Gupta. 'Mass Surveillance? You decide as per DoT's RTI responses #SaveOurPrivacy' (Internet Freedom Foundation, 16 June 2020) accessed 24 March 2022

public sectors, without recourse to remedy, against the backdrop of growing surveillance impunity.

51. Despite the lack of an effective data protection regime that safeguards people's rights, the government has been accelerating proposals for projects entailing massive exercises of collection and retention of personal information, including for example, a digital health ID[92], a model of "federated digital identities"[93], and linking of Aadhar with voter IDs[94]. This is contrary to the underlying purpose of the imminent personal data protection framework, and severely undermines people's right to privacy and freedom of choice with respect to their data.

52. The current draft of the Personal Data Protection Bill in India, with recommendations in the Joint Parliamentary Committee report, fails to adequately uphold international standards and best practices[95], human rights principles[96] and safeguards aligned with the rulings of the Indian Supreme Court on the right to privacy[97].

53. The draft data protection law also deviates from the positive recommendations and privacy protections[98] envisaged in the report of the Justice Srikrishna Committee[99] that spearheaded the process of devising a personal data protection framework for India in 2018.

54. At present, India has a draft data protection law that jeopardizes privacy, and fails to: (a) create a data protection authority with complete independence from the government; (b) initiate surveillance reform, impose restrictions and establish an independent oversight mechanism to ensure accountability and transparency; (c) impose meaningful limitations and safeguards, in line with principles of necessity and proportionality, on the government's extensive powers to access and control data; and (d) engender a data protection regime that empowers people to exercise and enforce their fundamental rights. The

---

[92] Live Mint, *Digital Health ID Card for Every India: Five Points Explained*, 27 September 2021, https://www.livemint.com/news/india/digital-health-id-card-for-every-indian-5-key-points-explained-11632715587318.html

[93] https://indianexpress.com/article/india/it-ministry-plan-one-digital-id-that-links-7747828/

[94] https://rethinkaadhaar.in/blog/voteridaadhaarlinkage

[95] See Access Now, *Creating a Data Protection Framework: A Do's and Dont's Guide for Lawmakers*, https://www.accessnow.org/cms/assets/uploads/2019/11/Data-Protection-Guide-for-Lawmakers-Access-Now.pdf

[96] Necessary & Proportionate: International Principles on the Application of Human Rights to Communications Surveillance, https://necessaryandproportionate.org/files/en_principles_2014.pdf.

[97] Privacy International, Stakeholder Report, Universal periodic Review - 27th Session, *The Right to Privacy in India,* https://privacyinternational.org/sites/default/files/2018-04/India_UPR_Stakeholder%20Report_Right%20to%20Privacy.pdf

[98] https://www.moneycontrol.com/news/business/data-protection-bill-is-orwellian-loaded-in-favour-of-the-government-justice-bn-srikrishna-7763331.html

[99] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, *A Free and Fair Digital Economy Protecting Privacy, Empowering Indians* https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf

Bill must be amended, in consultation with all stakeholders, including civil society, before it can be implemented as a rights respecting law.

55. Data protection requirements around purpose limitation, free, explicit, prior and informed consent for data processing, data minimisation, and integrity and confidentiality of data are even more critical for people who face lateral surveillance and for whom the exploitation of their data can have more severe implications for their rights to privacy, security and other fundamental rights. For instance, the risk of processing of personal data for individual profiling leading to discrimination on the grounds of sexual orientation, gender identity, gender expression and sex characteristics is only growing as digital identity programmes are becoming mandatory in many parts of the world.

56. Further, this crucial legislative vacuum exacerbates the damage caused by data breaches owing to lack of recourse for those affected. In 2021, India ranked third in the world in terms of number of data breaches, with a total of 86.[100] 63 million Indian users' data breached till November 2021.[101] There is insufficient investigation and prosecution of such data breaches, and a lack of any meaningful effort from the executive to ensure that individuals have avenues to seek remedy and redressal for violation of their rights.

(iii) Violations of the Right to Privacy of Transgender Persons

57. Going against the decisions of the Supreme Court in *NALSA v Union of India*[102] and *Puttaswamy v. Union of India*[103] (which recognised right to privacy as a fundamental right), the Transgender Persons (Protection of Rights) Act, 2019[104] continues to medicalise transgender persons by demanding a medical certificate from individuals who wish to identify within the binary genders of male and female. This limits the ability of every individual to exercise their bodily autonomy in changing their name and gender on identification documents, enter data systems and access any of their rights. Further this also affects the privacy of transgender persons. The medical process has been challenged in the legal petition against the new law.[105]

58. The access to any state-sanctioned welfare programme, public sector or private sector services all require transgender individuals to become a part of different data systems using a government-issued identification document in a

---

[100] https://www.businesstoday.in/latest/trends/story/india-ranks-third-in-global-data-breaches-in-2021-report-315750-2021-12-15#:~:text=Not%20much%2C%20if%20you%20are,its%20own%20breach%20detection%20mechanism.

[101] Ibid.

[102] (2014) 5 SCC 438

[103] (2017) 10 SCC 1

[104] Transgender persons (Protection of Rights) Act, 2019, https://www.indiacode.nic.in/handle/123456789/13091?sam_handle=123456789/1362

[105] Center for Law and Policy Research, *Grace Banu Ganeshan & Ors. v. Union of India & anr.* | *A constitutional challenge to The Transgender Persons (Protection of Rights) Act 2019*, https://clpr.org.in/litigation/grace-banu-ganesan-ors-v-union-of-india-anr/

person's preferred name and self-identified gender as transgender. Unless an individual discloses their transgender identity, they cannot access exclusive programmes for transgender persons.[106] Individuals are required to repeatedly reveal and provide their identity; and constantly expected to choose between their right to life — public healthcare, welfare schemes and their right to privacy.

59. With policies still underway for inclusion of transgender persons, existing digital systems and the digital processes to access them, continue to remain inaccessible to transgender persons in terms of gender category, technical understanding, usability, language, and interface, among others.[107]

VIII. RECOMMENDATIONS

60. We recommend that the Government of India take the following measures to uphold human rights online in India:

Internet Shutdowns

- Refrain from intentionally slowing, blocking, or shutting down internet and telecommunications services, websites or applications and ensure that due processes established by law and court judgments are strictly followed, with a robust mechanism for redressal and remedy.
- Publish internet shutdown orders.
- Maintain a database of internet shutdown orders issued across the country.
- Conduct a study to examine the effectiveness of internet shutdown orders in dealing with law and order situations.
- Amend the 2017 Rules and provide for a Review Committee which consists of former judges of the High Court or the Supreme Court, and empower the Committee to set aside internet shutdown orders.

Digital Exclusion

- Implement comprehensive social auditing and policy analysis of the different Artificial Intelligence frameworks; and ensure that when such AI systems are used, that redressal mechanisms are put in place that do not put the burden on the welfare beneficiaries.

Freedom of Speech Online

---

[106] Jurist, *Restoring Dignity: Nuances of Transgender Rights in India*, 12 October 2020,https://www.jurist.org/commentary/2020/10/ayush-mishra-transgender-india/
[107] Brindalakshmi K., *Gendering of Development Data in India - Beyond the Binary*, https://cis-india.org/raw/brindaalakshmi-k-gendering-development-data-india

- Repeal or amend laws and regulations, including Section 124A of the Indian Penal Code and the Unlawful Activities (Prevention) Act, 1967, which restrict freedom of expression and bring them in line with international human rights law.
- Withdraw all cases against individuals facing harassment, intimidation and prosecution from state authorities for legitimate expression and dissent against the government.

Technology-facilitated gender-based violence & Hate Speech

- Amend laws addressing hate speech that constitutes incitement to discrimination, hostility, or violence, to bring them in line with international human rights standards and ensure that they are not misused to undermine freedom of expression of minorities, while holding accountable those engaging in incitement to discrimination, hostility and violence against them.
- Develop appropriate mechanisms of accountability for social media platforms and other technology companies to ensure that hate speech and gender-based violence is regulated on their platforms, there is appropriate response to such instances and safeguards and redressal mechanisms are available for those affected.
- Review and strengthen policies, legal and regulatory frameworks to address gender-based violence violence in digital contexts.

Privacy, Surveillance & Data Protection

- Adopt an intersectional approach to protecting the right to privacy, which recognises the specific experiences and threats to privacy experienced by women and LGBTIQ persons; and amend the Transgender Persons (Protection of Rights) Act, 2019 to ensure the right to privacy of trans persons.
- Pass a comprehensive law on informational privacy and surveillance, which strongly regulates state-sponsored surveillance and imposes limitations in line with necessity and proportionality on access to data and interception of communications, under judicial control and independent oversight, and with other protections to safeguard citizens.
- Implement a data protection framework that establishes a data protection authority with complete independence from the executive, creates meaningful checks against the government's powers to access data, and clear and enforceable rights for individuals with respect to the collection and use of their data.

ANNEX

Recent Cases of Surveillance & Spyware Harms

(i) **Use of Pegasus spyware to target journalists, politicians and human rights defenders in India**: In July 2021, the Wire[108], as part of an international collaborative investigation titled "Pegasus Project", revealed that numerous journalists, politicians and human rights defenders in India were targeted through the use of NSO Group's Pegasus spyware. Once Pegasus has been installed in the mobile device, it can harvest SMS messages, address books, call history, calendars, emails and internet browsing histories as well as gain access to and extract any files on the device. No such power to hack the phones of Indian citizens exists under Indian law, and the pre-existing surveillance powers available under the Telegraph Act, 1885 and the Information Technology Act, 2000 do not permit the installation of spyware or hacking mobile devices. Hacking of computer resources, including mobile phones and apps, is in fact a criminal offence under the Information Technology Act, 2000.

(ii) **Use of NetWire against the accused in the Bhima Koregaon case**: Reports[109] by a digital forensics consulting company named Arsenal Consulting reveal that a commercially available malware named NetWire was used to surveil and plant evidence on the computers of two of the accused in the Bhima Koregaon case. The reports relate specifically to two of the accused, Rona Wilson (Reports 1[110] & 2[111]) and Surendra Gadling (Report 3[112]). According to the reports, both Rona Wilson's and Surendra Gadling's computers were compromised for 22 and 20 months respectively. The primary goals of the attacker were surveillance and incriminating document delivery. In their report, Arsenal has indicated that this is one of the most serious cases involving evidence tampering that they have ever encountered, based on various metrics which include the vast timespan between the delivery of the first and last incriminating documents on multiple defendants' computers.

(iii) **Indian hack-for-hire firm BellTrox banned from Facebook for surveillance activities**: On December 16, 2021, Meta, which is the parent company of Facebook, issued a press release titled, "Taking Action Against the Surveillance-For-Hire Industry"[113]. This press release was on the basis of and accompanied by a threat report titled, "Threat Report on the Surveillance-for-Hire Industry"[114]. At the end of a months-long investigation, seven entities were identified as engaging in surveillance-for-hire activities and subsequently removed from Meta's platforms. One of the entities identified was the Delhi-based M/s Belltrox Infotech Services Private

---

[108] Siddharth Varadarajan, 'Pegasus Project: How Phones of Journalists, Ministers, Activists May Have Been Used to Spy On Them' (The Wire, 18 July 2021) accessed March 24, 2022
[109] Arsenal, 'BK Case' (Arsenal, 18 Dec 2021) accessed 24 March 2022
[110] Arsenal, 'Report I - Rona Wilson' (Arsenal, 18 December 2021) accessed 24 March 2022
[111] Arsenal, 'Report II - Rona Wilson' (Arsenal, 18 December 2021) accessed 24 March 2022
[112] Arsenal, 'Report III - Surendra Gadling' (Arsenal, 18 December 2021) accessed 24 March 2022
[113] David Agranovich and Mike Dvilyanski, 'Taking Action Against the Surveillance-For-Hire Industry', (Meta, 16 December 2021) accessed 24 March 2022
[114] Mike Dvilyanski, David Agranovich and Nathaniel Gleiche, Threat Report on the Surveillance-for-Hire Industry', (Meta, 16 December 2021) accessed 24 March 2022

Limited (“Belltrox”). According to the threat report, Meta has removed about 400 Facebook accounts linked to Belltrox, the vast majority of which were inactive for years. Belltrox was engaged in reconnaissance of, engagement with, and exploitation of targets. According to the threat report, Meta has removed about 400 Facebook accounts linked to Belltrox, the vast majority of which were inactive for years. Previously, CitizenLab[115] and Reuters[116] have also disclosed the information about Belltrox’s hacking activities. The techniques adopted by them included phishing attacks and impersonation of persons, which they used to either hack into devices and get access to private data or deceive people into sharing their private data.

Recent Cases of Mass Surveillance

(i) The National Automated Facial Recognition System[117] (AFRS) aims to develop and use a national database of photographs which is to be used in conjunction with a facial recognition technology (FRT) system by Central and State security agencies. However, use of FRT has been increasing steadily in the past few years, especially by State Police departments, such as, among others, the Delhi Police[118], the Hyderabad Police[119], the Punjab Police[120], the Bengaluru Police[121], the Maharashtra Police[122] and the Tamil Nadu Police[123]. Claims relating to accuracy of FRT systems are routinely exaggerated and the real numbers leave much to be desired. The implementation of such faulty FRT systems would lead to high rates of false positives, leading to misidentification, and false negatives, leading to exclusion, in this recognition process. While there have been claims of a fully accurate FRT system, none of these claims have been corroborated by independent review and audit. The National Institute of Standards and Technology (NIST) has extensively tested FRT systems for 1:1 verification and 1:many identification and how accuracy of these systems vary across demographic groups.[124] These independent studies have concluded that currently, no FRT system has 100% accuracy. An accurate FRT system would hypothetically have a 100% success rate in 1:1 verification and/or 1:many identification. However, it will come with its own ominous connotations, the most problematic of which may be state led mass surveillance and difficulty for outside actors to counter-challenge government decisions. Mass surveillance is also effectuated through the use of CCTV cameras, sometimes in conjunction with FRT, by State Police departments to surveill the entire population of specific cities. Recently, the Government of the National Capital Territory of Delhi boasted about

[115] John Scott-Railton, Adam Hulcoop, Bahr Abdul Razzak, Bill Marczak, Siena Anstis, and Ron Deibert, ‘Dark Basin: Uncovering a Massive Hack-For-Hire Operation’, (The Citizen Lab, 9 June 2020) accessed 24 March 2022
[116] Jack Stubbs, Raphael Satter, and Christopher Bing ‘Exclusive: Obscure Indian cyber firm spied on politicians, investors worldwide’ (Thomson Reuters, 9 June 2020) accessed 24 March 2022
[117] Anushka Jain, ‘NCRB's National Automated Facial Recognition System’ (Panoptic Tracker, 15 March 2022) accessed 24 March 2022
[118] Anushka Jain, ‘Delhi Police’ (Panoptic Tracker, 23 February 2018) accessed 24 March 2022
[119] Anushka Jain, ‘Hyderabad Police’ (Panoptic Tracker, 28 January 2021) accessed 24 March 2022
[120] Anushka Jain, ‘Punjab Police’ (Panoptic Tracker, 16 February 2021) accessed 24 March 2022
[121] Anushka Jain, ‘Bengaluru Police’ (Panoptic Tracker, 9 March 2022) accessed 24 March 2022
[122] Anushka Jain, ‘Maharashtra Police’ (Panoptic Tracker, 16 November 2020) accessed 24 March 2022
[123] Anushka Jain, ‘Tamil Nadu Police’ (Panoptic Tracker, 08 February 2020) accessed 24 March 2022
[124] Patrick Grother, Mei Ngan and Kayee Hanaoka, ‘Ongoing Face Recognition Vendor Test (FRVT) Part 1: Verification’ (National Institute of Standards and Technology, 19 November 2019) accessed 24 March 2022

New Delhi being the most surveilled city in the world with 1,826.6 cameras per square mile.[125] However, multiple studies, through the years, have proven that CCTV surveillance has little to no effect on reduction of crime in the surveilled area.[126]

(ii) The National Intelligence Grid[127] (NATGRID) is an integrated IT solution which would allow user agencies to access data gathered from various databases such as credit and debit cards, tax, telecom, immigration, airlines and railway tickets, passports, driving licences among others. The Right to Information Act, 2000 which aims to bring transparency and accountability to government authorities contains a provision which exempts intelligence agencies from its purview under S.24(2) of the Act.[128] NATGRID is exempted from the RTI Act, 2005 vide Gazette of India Notification No. GSR 442 (E) dated 09.06.2011 issued by DOP&T.[129] In addition to being exempt from the RTI Act, NATGRID is also being developed and deployed in the absence of a data protection law in India. Since NATGRID aims to collate data from various sources to create profiles of people to track for criminal activity, it is necessary that data protection measures be put in place to ensure that NATGRID does not violate its mandate by suffering from function creep. “Function creep” occurs when information is used for a purpose that is not the original specified purpose. In the absence of data protection measures and by being exempt from disclosures under the RTI Act, NATGRID presents the very obvious danger of becoming a tool for state-sponsored mass surveillance.

(iii) The Centralised Monitoring System[130] (CMS) is an ambitious surveillance system that monitors text messages, social-media engagement and phone calls on landlines and cell phones, among other communications. In the absence of a data protection law in India and without any intermediaries in place, the process through which interception would be done under the CMS lacks transparency. This means that the general public will not know if and when a person’s data has been intercepted. It would also be difficult to ascertain whether there was a valid reason for this interception. A practice of mass surveillance could be adopted wherein large groups of people have their data intercepted without a valid reason. Since these interception authorisations will be done by the government agencies internally, there will be no way of knowing about them and whether they were done for a valid reason, let alone questioning or challenging them. Further, Right To Information (‘RTI’) applications filed by the Internet Freedom Foundation (‘IFF’) reveal that the Department of Telecommunications (‘DOT’) has sought bulk Call Data Records from telecom operators.[131]

---

[125] Aam Aadmi Party, ‘Delhi is now World's No. 1 City with most CCTV cameras per square mile!’ (Twitter, 26 August 2021) accessed 24 March 2022
[126] NO CCTV - The case against - Reports’ (No CCTV) accessed 24 March 2022
[127] D. Haritha and Ch Praneeth, ‘National intelligence grid — An information sharing grid’ (IEEE, 14 December 2017) accessed 24 March 2022
[128] Right to Information 2005, s 24
[129] Department of Personnel and Training, Gazette of India, Extraordinary, Part II, section-3 sub-section (i) (Notification, 9 June 2011)
[130] Department of Telecommunications, Amendment to the Unified License agreement regarding Central Monitoring System (Amendment 2 of 2013, 11 October 2013) accessed 24 March 2022
[131] Apar Gupta. ‘Mass Surveillance? You decide as per DoT’s RTI responses #SaveOurPrivacy’ (Internet Freedom Foundation, 16 June 2020) accessed 24 March 2022

(iv) The Crime and Criminal Tracking Network System (CCTNS) aims to connect police stations across the country to increase ease of access to data related to FIR registration, investigation and chargesheets in all police stations. CCTNS is being implemented in the country without a data protection law in place. This leads to privacy concerns because the CCTNS is proposed to be integrated with various projects such the NATGRID and AFRS. Integration of the CCTNS with these projects would thus allow the state to create complete profiles of citizens.