The Dialogue®
INFORM ENGAGE IDEATE

December, 2024

Cyber Safety Handbook for Members of the Indian Parliament

Cyber Safety Handbook for Members of the Indian Parliament

Copyeditor and Thematic Designer:
Akriti Jayant (Head of Communications, The Dialogue)

The Dialogue™ is a public policy think tank with a vision to drive a progressive narrative in India's policy discourse. Founded in 2017, we believe in facilitating well-researched policy debates at various levels to help develop a more informed citizenry, on areas around technology and development issues. The Dialogue™ has been ranked as the world's Top 10 think tanks to watch out for, by the Think Tank and Civil Societies Programme (TTCSP), University of Pennsylvania in their 2020 and 2021 rankings.

For more information Visit thedialogue.co

Suggested Citation
Cyber Safety Handbook for Members of the Indian Parliament. (December 2024). The Dialogue.

Catalogue No
TD/PR/HB/1224/01

Publication Date
December 11, 2024

TABLE OF CONTENTS

I. Introduction

1.1. Problem Statement

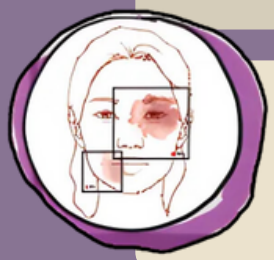
Imagine a retired teacher grappling with the shock of fraudulent loans taken in her name, a teenager facing the crushing toll of cyberstalking, or a small business owner watching their hard-earned savings vanish from a hacked UPI account. These are not isolated incidents—they are part of an alarming trend that touches every corner of our country, from bustling cities to rural villages. With over 900 million digital nagriks connected to the internet [1], these incidents are increasingly affecting individuals across the country, manifesting in the following ways:

Financial Frauds

In early 2024, Indians lost ₹1,750 crore to cyber fraud, with ₹120.3 crore from "digital arrest" scams[2]. The National Cybercrime Reporting Portal received 7.4 lakh complaints, mostly related to online investment fraud, gaming apps, and algorithm manipulation. By May 2024, daily complaints averaged 7,000, with 85% involving financial fraud.

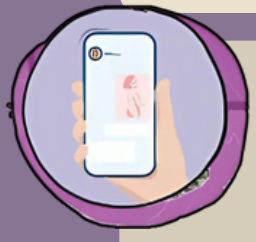
India Leads in CSAM Reports in 2022

- India received 5,675,324 reports from the NCMEC CyberTipline in 2022, the highest globally[3].
- Of the 32 million global reports on child sexual abuse material (CSAM), 5.6 million were uploaded by perpetrators based in India.[4]



Technology-Facilitated Abuse Against Women on the Rise

- Tech-facilitated abuse against women rose 11% in 2022[5].
- Maharashtra reported the most online stalking and bullying cases in 2022[6].
- Crimes included NCII, blackmail, defamation, morphing, and fake profiles.



Extortion Scams

- WFH and part-time job scams topped cybercrime reports in 2023.[7]
- Illegal lending apps ranked second, exploiting users with hidden fees and blackmail.
- Sextortion cases, often underreported, reached 19,000 in 2023.

Massive Data Breach Exposes Personal Information

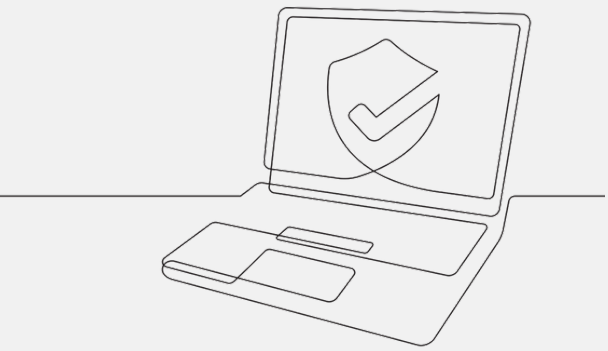
India ranked 5th globally for the most breached countries in 2023, with 5.3 million leaked accounts[8].

The Ripple Effects Threaten Both Individual Safety and National Security

A Member of Parliament is well placed to address challenges at the intersection of legislative reform and community engagement. Constituents look to their representatives not only for the enactment of legislation but also for visionary leadership in navigating the evolving digital landscape. Whether it involves combating cyber fraud, protecting vulnerable populations, or ensuring the responsible adoption of digital technologies, the insights and actions of an MP play a pivotal role in shaping India's path toward a secure and inclusive digital economy.

Cyber incidents are not confined to individuals; their consequences ripple across sectors, eroding trust, disrupting operations, and threatening national security

1.2. Why Prioritise Cyber Safety



CONSTITUENT SAFETY

Cybercrime affects the mental health, privacy, and financial security of citizens.

IMPROVING PUBLIC TRUST IN TECHNOLOGY

Cyber safety becomes key to maintaining public trust in technology and promoting responsible use of digital platforms.

BROADER SOCIAL AND ECONOMIC IMPLICATIONS

Unsafe digital environments discourage citizens from engaging in online platforms, slowing economic growth in critical areas like e-commerce, digital banking, and education, particularly in rural and underserved areas.

1.3. Purpose of the Handbook

This handbook has been thoughtfully designed to assist esteemed Parliamentarians in navigating the complexities of online safety. It offers actionable strategies and real-world examples on utilising Parliamentary Interventions and Civic Engagement Mechanisms to facilitate discussions on online safety, both within Parliament and in your respective constituencies and tackle vital issues such as technology-facilitated gender violence (TFGBV), financial scams, the digital literacy gap, and the infrastructural divide, among others.

1.4. How to Use It

This handbook is intended to serve as a resource that Parliamentarians can refer to as they address pressing online safety concerns in their legislative work and constituency outreach efforts.

For new Parliamentarians

It offers a foundational understanding of cyber threats and provides tools for drafting informed policies to enhance online safety.

For seasoned lawmakers

It serves as a reflective guide, offering insights to refine and strengthen ongoing efforts in combating digital challenges.

It is not necessary to go through the document in a linear fashion. Instead, Parliamentarians are encouraged to focus on the sections most relevant to their immediate needs or areas of interest. The handbook is structured into key sections that include:

- **Understanding Legal Framework and Policies on Cyber Safety**: A comprehensive overview of the essential legal frameworks and opportunities for actions surrounding cyber safety.
- **Leveraging Parliamentary Interventions:** Guidance on using parliamentary devices such as Private Member Bills, Question Hour, and Zero Hour to raise and address urgent cyber safety issues.
- **Civic Engagement and Participation Opportunities:** Practical approaches to engage constituents and raise awareness about online safety concerns, fostering a safer digital environment in communities.

Each section is enriched with real-world examples, offering Parliamentarians a valuable repository of solutions that have worked in other contexts, inspiring actionable and impactful efforts in their constituencies.

1.5. KEY ACTION AREAS FOR CYBER SAFETY

As representatives of the people, Members of Parliament have a critical role in ensuring a safe, inclusive, and equitable digital environment. Below are key areas to consider for fostering cyber safety and empowering constituents in the digital age:

Access: Ensuring Equitable Technology Access for All

- Consider supporting initiatives that address the digital divide and the denial of technology as a form of violence, particularly for marginalised groups, including women and gender minorities.
- Explore opportunities to establish public Wi-Fi zones or digital resource centres to provide equitable access, particularly during crises or emergencies.

Prevention: Shaping Societal Norms for Safer Digital Spaces

- Support campaigns that promote awareness about gender-based stereotypes and encourage respectful behaviour online.
- Collaborate with schools, NGOs, and community organisations to integrate digital literacy and online safety education, fostering healthier perceptions of technology use.

Early Intervention: Empowering Communities to Address Risks

- Promote targeted programs for vulnerable groups, including women and children, such as digital literacy workshops to help them identify and report online threats.
- Encourage tech companies to adopt safety-by-design measures, such as abuse detection tools and privacy settings tailored to these groups, providing early protection against cyber risks.

Response and Redressal: Strengthening Support Mechanisms

- Support for accessible and confidential mechanisms for reporting cybercrimes, ensuring victims feel safe and supported.
- Work towards improving the responsiveness of legal systems to provide timely justice and resolution for victims of online abuse.

Recovery and Healing: Supporting Survivors in Rebuilding Confidence

- Facilitate access to counselling and mental health services for survivors of cyber abuse to support their recovery journey.
- Encourage partnerships and funding for local organisations to provide comprehensive care and empowerment programs for survivors.

Research: Promoting Data-Driven Solutions for Cyber Threats

- Encourage research initiatives that collect and analyse data on online abuse to better understand its patterns and impacts.
- Support the use of this data to inform targeted strategies and policymaking, addressing the specific needs of vulnerable groups.

1.6. How to Select and Implement Parliamentary Devices and Civic Engagement Mechanisms

Choosing and prioritising the right parliamentary devices and civic engagement mechanisms is essential for addressing the complexities of cyber threats. Here is a step-by-step approach that MPs can use to choose and implement these devices and mechanisms strategically.

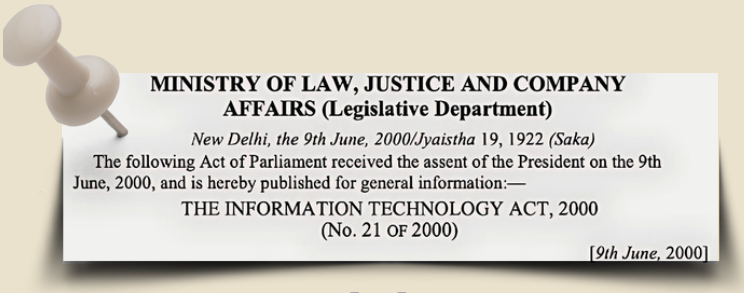
II. Legal Framework and Policies for Cyber Safety

India's policy landscape for technology is undergoing a dynamic transformation, particularly in cyber safety and digital access. Flagship initiatives like Digital India and BharatNet have expanded internet connectivity to millions, bridging the digital divide. However, ensuring robust cybersecurity and equitable access remains critical.

The Digital Personal Data Protection Act, 2023[14] is a key step in safeguarding user data, but its operationalisation depends on robust rules. The proposed Digital India Act aims[15] to replace the Information Technology Act, 2000,[16] addressing challenges like misinformation, intermediary liability, and platform accountability. Similarly, the National Cybersecurity Policy[17] and National IT Policy,[18] both over a decade old, require updates to combat advanced threats and align with emerging technologies.

Efforts to establish an AI Safety Institute underscore the government's focus on ethical AI development as part of the India AI mission.[19] Regulatory frameworks for online gaming and IT Rules are also evolving to tackle harms like addiction, harmful content and cyber frauds.[20]

Parliamentarians are actively shaping India's digital governance through various interventions and initiatives. As online challenges grow more complex, their role in addressing existing gaps and emerging issues becomes increasingly important. Through strategic legislative reforms and community engagement, MPs can drive meaningful and lasting change for both their constituents and the broader digital ecosystem.



MINISTRY OF LAW, JUSTICE AND COMPANY AFFAIRS (Legislative Department)

New Delhi, the 9th June, 2000/Jyaistha 19, 1922 *(Saka)*

The following Act of Parliament received the assent of the President on the 9th June, 2000, and is hereby published for general information:—

THE INFORMATION TECHNOLOGY ACT, 2000
(No. 21 OF 2000)

[*9th June*, 2000]

1. Information Technology (IT) Act, 2000 and IT Rules, 2021

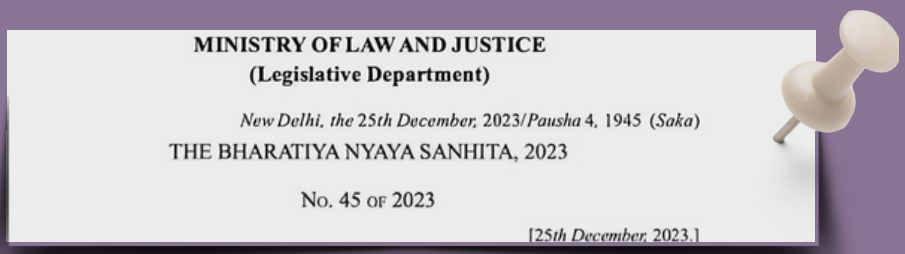
The IT Act, 2000 and IT Rules, 2021 address critical aspects of electronic communication, cybercrime, digital content regulation, platform accountability, privacy, and user protection. Their overarching goal is to safeguard users while fostering a regulated online ecosystem. Opportunities for improvement include:

Tackling Emerging Harms

Focus on legislative and policy considerations for addressing new-age harms, such as AI-generated NCII and CSEAM.

Empowering Law Enforcement

Support funding for capacity-building programs that include gender-responsive training for law enforcement to enhance response mechanisms.



MINISTRY OF LAW AND JUSTICE
(Legislative Department)

New Delhi, the 25th December, 2023/*Pausha* 4, 1945 (*Saka*)

THE BHARATIYA NYAYA SANHITA, 2023

No. 45 OF 2023

[*25th December*, 2023.]

2. Bharatiya Nyaya Sanhita (BNS), 2023

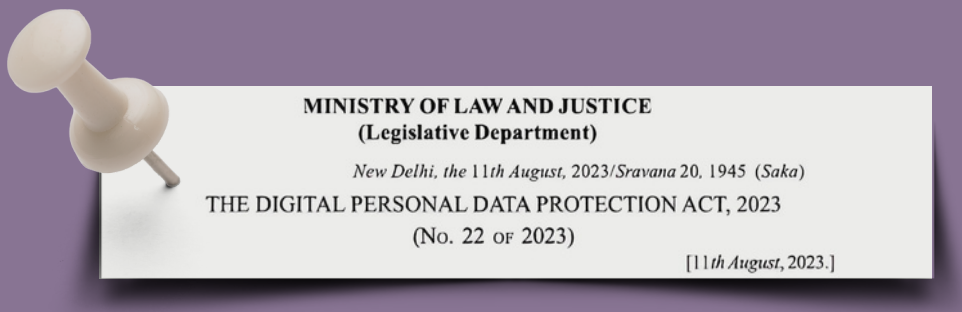
The Bharatiya Nyaya Sanhita (BNS) replaces the Indian Penal Code, aiming to reform the criminal justice system to align with contemporary crime trends. However, despite this reform, it falls short of addressing modern digital crimes due to the absence of clear definitions for cybercrimes and the lack of inclusivity. Opportunities for improvement include:

Community Education Initiatives

Promote collaboration between community organisations and law enforcement to implement localised safety awareness programs that educate all genders on the risks of technology-facilitated violence.

Provisions Addressing Sexual Violence Against Men and Trans Persons

Focus on policy considerations for the inclusion of provisions to explicitly address sexual violence against adult men and trans persons in the BNS.



MINISTRY OF LAW AND JUSTICE
(Legislative Department)

New Delhi, the 11*th August*, 2023/*Sravana* 20, 1945 (*Saka*)

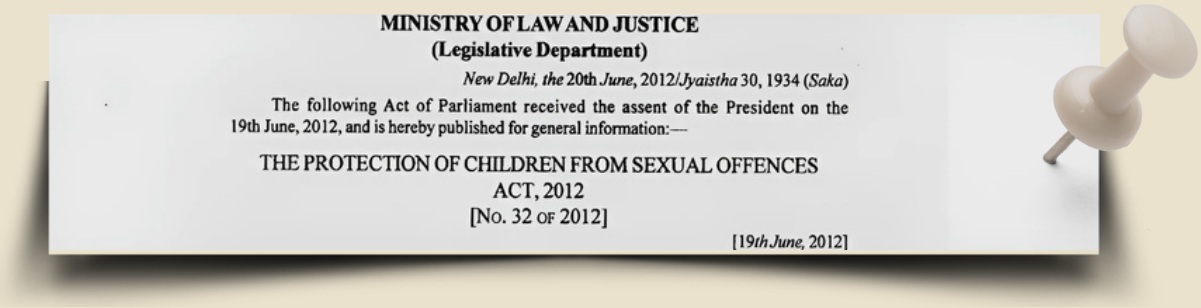
THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023
(No. 22 OF 2023)

[11*th August*, 2023.]

3. Digital Personal Data Protection Act (DPDPA), 2023

The DPDP Act establishes a framework for personal data processing, emphasising data accuracy, security, and user rights. Opportunities for improvement include:

Raise Awareness	Ensure Effective Implementation
Collaborate with digital literacy NGOs to launch awareness campaigns educating citizens about their privacy rights under the DPDP Act.	Promote regular reviews and enhancements of grievance redressal mechanisms to adapt to the ever-evolving digital landscape.



MINISTRY OF LAW AND JUSTICE
(Legislative Department)

New Delhi, the 20th *June*, 2012/*Jyaistha* 30, 1934 (*Saka*)

The following Act of Parliament received the assent of the President on the 19th June, 2012, and is hereby published for general information:—

THE PROTECTION OF CHILDREN FROM SEXUAL OFFENCES ACT, 2012
[No. 32 OF 2012]

[19*th June*, 2012]

4. Protection of Children from Sexual Offences (POCSO) Act, 2012

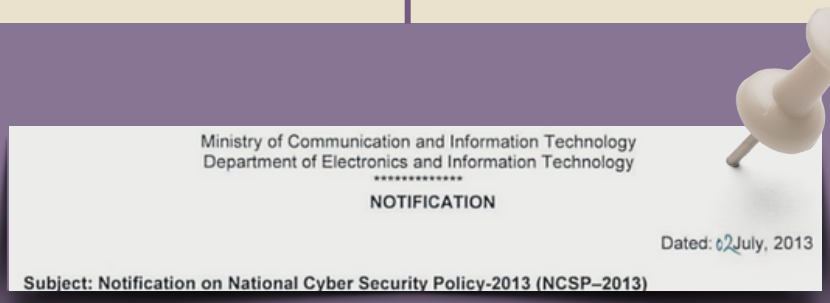
The POCSO Act criminalises exploitative content involving minors but requires updates to tackle new-age threats. Opportunities for improvement include:

Modernise Terminology	Drive School Campaigns
Adopt globally recognised terms like "Child Sexual Exploitation and Abuse Material (CSEAM)" to align with international standards and enhance legal and policy coherence.	Partner with schools to develop age-appropriate online safety programs, emphasising early interventions to protect children from online risks.

5. National Education Policy (NEP), 2020

The NEP emphasises digital literacy to equip future generations with the tools for safe technology navigation. Opportunities for improvement include:

Promote Cyber Safety Education	Ensure Universal Access
Incorporate cyber safety into school curricula, leveraging cross-stakeholder collaboration to design comprehensive and inclusive content.	Collaborate with rural development organisations to deliver equitable digital literacy programs, reaching underserved communities effectively.


Ministry of Communication and Information Technology
Department of Electronics and Information Technology
NOTIFICATION
Dated: 02July, 2013
Subject: Notification on National Cyber Security Policy-2013 (NCSP–2013)

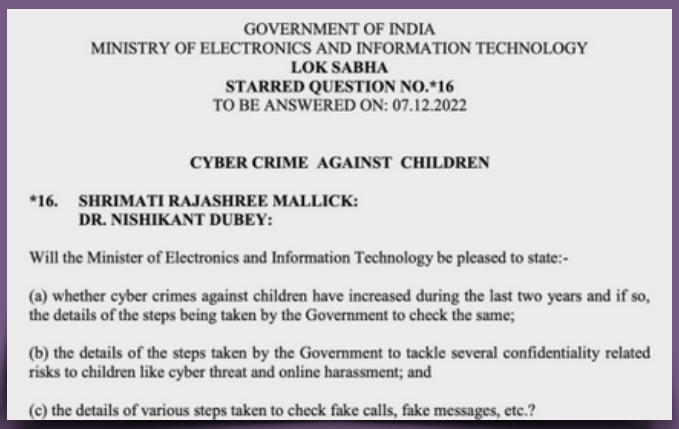
6. National Cyber Security Policy, 2013

This policy serves as a framework for safeguarding India's digital infrastructure but requires urgent updates. Opportunities for improvement include:

Call for Reform	Foster Multistakeholder Collaboration
Advocate for updated frameworks that incorporate contemporary threats like ransomware and address nation-state-sponsored cyberattacks.	Engage tech companies, policymakers, and NGOs in dialogues to inform and implement effective reforms.

III. Legislative Strategies and Parliamentary Devices

Effective legislative action is vital for addressing the growing challenges of cyber threats in India. Parliamentarians are well-placed to drive these efforts by leveraging a range of parliamentary devices to champion cyber safety reforms, hold the government accountable, and ensure robust policy implementation.



GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
STARRED QUESTION NO.*16
TO BE ANSWERED ON: 07.12.2022

CYBER CRIME AGAINST CHILDREN

***16. SHRIMATI RAJASHREE MALLICK:**
DR. NISHIKANT DUBEY:

Will the Minister of Electronics and Information Technology be pleased to state:-

(a) whether cyber crimes against children have increased during the last two years and if so, the details of the steps being taken by the Government to check the same;

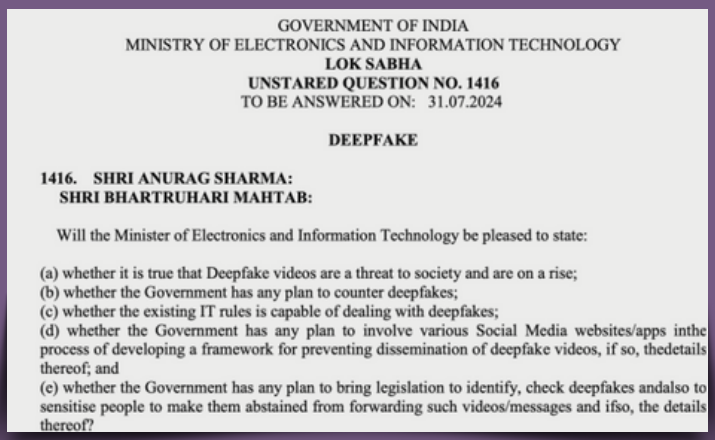
(b) the details of the steps taken by the Government to tackle several confidentiality related risks to children like cyber threat and online harassment; and

(c) the details of various steps taken to check fake calls, fake messages, etc.?

PARLIAMENTARY QUESTIONS

PURPOSE

Members can ask Ministers about laws, policies, and issues affecting their constituents, holding the government accountable for cyber safety issues.



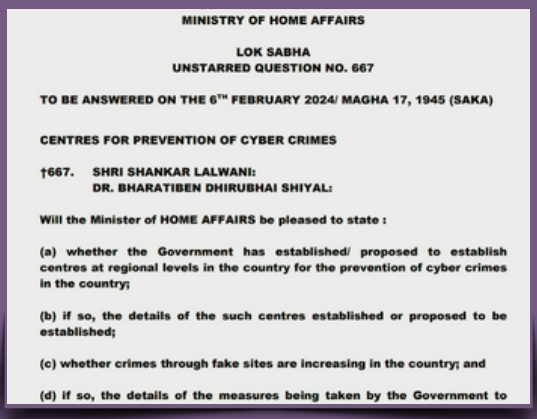
GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARED QUESTION NO. 1416
TO BE ANSWERED ON: 31.07.2024

DEEPFAKE

1416. SHRI ANURAG SHARMA:
SHRI BHARTRUHARI MAHTAB:

Will the Minister of Electronics and Information Technology be pleased to state:

(a) whether it is true that Deepfake videos are a threat to society and are on a rise;
(b) whether the Government has any plan to counter deepfakes;
(c) whether the existing IT rules is capable of dealing with deepfakes;
(d) whether the Government has any plan to involve various Social Media websites/apps inthe process of developing a framework for preventing dissemination of deepfake videos, if so, thedetails thereof; and
(e) whether the Government has any plan to bring legislation to identify, check deepfakes andalso to sensitise people to make them abstained from forwarding such videos/messages and ifso, the details thereof?



MINISTRY OF HOME AFFAIRS

LOK SABHA
UNSTARRED QUESTION NO. 667

TO BE ANSWERED ON THE 6TH FEBRUARY 2024/ MAGHA 17, 1945 (SAKA)

CENTRES FOR PREVENTION OF CYBER CRIMES

†667. SHRI SHANKAR LALWANI:
DR. BHARATIBEN DHIRUBHAI SHIYAL:

Will the Minister of HOME AFFAIRS be pleased to state :

(a) whether the Government has established/ proposed to establish centres at regional levels in the country for the prevention of cyber crimes in the country;

(b) if so, the details of the such centres established or proposed to be established;

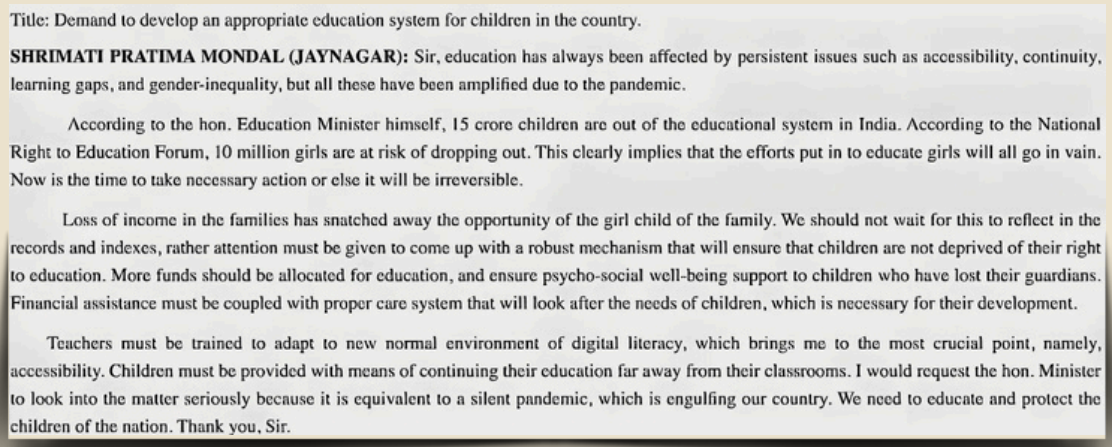
(c) whether crimes through fake sites are increasing in the country; and

(d) if so, the details of the measures being taken by the Government to

IMPACT

Parliamentary questions have driven attention to concerns like child safety, privacy, and platform accountability.[21.22.23]

ZERO HOUR



Title: Demand to develop an appropriate education system for children in the country.

SHRIMATI PRATIMA MONDAL (JAYNAGAR): Sir, education has always been affected by persistent issues such as accessibility, continuity, learning gaps, and gender-inequality, but all these have been amplified due to the pandemic.

According to the hon. Education Minister himself, 15 crore children are out of the educational system in India. According to the National Right to Education Forum, 10 million girls are at risk of dropping out. This clearly implies that the efforts put in to educate girls will all go in vain. Now is the time to take necessary action or else it will be irreversible.

Loss of income in the families has snatched away the opportunity of the girl child of the family. We should not wait for this to reflect in the records and indexes, rather attention must be given to come up with a robust mechanism that will ensure that children are not deprived of their right to education. More funds should be allocated for education, and ensure psycho-social well-being support to children who have lost their guardians. Financial assistance must be coupled with proper care system that will look after the needs of children, which is necessary for their development.

Teachers must be trained to adapt to new normal environment of digital literacy, which brings me to the most crucial point, namely, accessibility. Children must be provided with means of continuing their education far away from their classrooms. I would request the hon. Minister to look into the matter seriously because it is equivalent to a silent pandemic, which is engulfing our country. We need to educate and protect the children of the nation. Thank you, Sir.

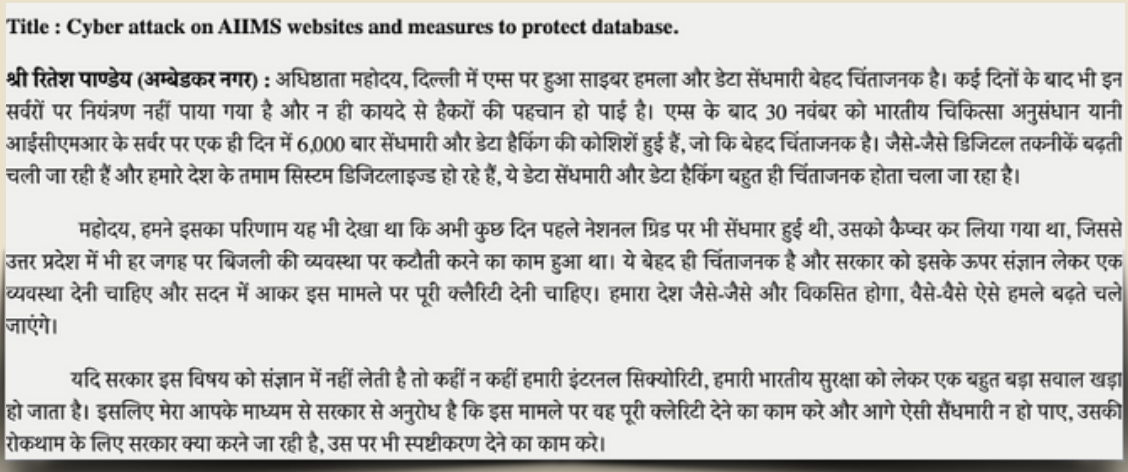
Lok Sabha; 13 December 2021

Purpose

Members can raise urgent public issues without prior notice, ensuring immediate government attention on critical matters like cybersecurity and digital safety.

Impact

Zero Hour discussions have sparked awareness and led to the implementation of targeted programs and regulatory reforms.[24,25]



Title : Cyber attack on AIIMS websites and measures to protect database.

श्री रितेश पाण्डेय (अम्बेडकर नगर) : अधिष्ठाता महोदय, दिल्ली में एम्स पर हुआ साइबर हमला और डेटा सेंधमारी बेहद चिंताजनक है। कई दिनों के बाद भी इन सर्वरों पर नियंत्रण नहीं पाया गया है और न ही कायदे से हैकरों की पहचान हो पाई है। एम्स के बाद 30 नवंबर को भारतीय चिकित्सा अनुसंधान यानी आईसीएमआर के सर्वर पर एक ही दिन में 6,000 बार सेंधमारी और डेटा हैकिंग की कोशिशें हुई हैं, जो कि बेहद चिंताजनक है। जैसे-जैसे डिजिटल तकनीकें बढ़ती चली जा रही हैं और हमारे देश के तमाम सिस्टम डिजिटलाइज्ड हो रहे हैं, ये डेटा सेंधमारी और डेटा हैकिंग बहुत ही चिंताजनक होता चला जा रहा है।

महोदय, हमने इसका परिणाम यह भी देखा था कि अभी कुछ दिन पहले नेशनल ग्रिड पर भी सेंधमार हुई थी, उसको कैप्चर कर लिया गया था, जिससे उत्तर प्रदेश में भी हर जगह पर बिजली की व्यवस्था पर कटौती करने का काम हुआ था। ये बेहद ही चिंताजनक है और सरकार को इसके ऊपर संज्ञान लेकर एक व्यवस्था देनी चाहिए और सदन में आकर इस मामले पर पूरी क्लैरिटी देनी चाहिए। हमारा देश जैसे-जैसे और विकसित होगा, वैसे-वैसे ऐसे हमले बढ़ते चले जाएंगे।

यदि सरकार इस विषय को संज्ञान में नहीं लेती है तो कहीं न कहीं हमारी इंटरनल सिक्योरिटी, हमारी भारतीय सुरक्षा को लेकर एक बहुत बड़ा सवाल खड़ा हो जाता है। इसलिए मेरा आपके माध्यम से सरकार से अनुरोध है कि इस मामले पर वह पूरी क्लेरिटी देने का काम करे और आगे ऐसी सैंधमारी न हो पाए, उसकी रोकथाम के लिए सरकार क्या करने जा रही है, उस पर भी स्पष्टीकरण देने का काम करे।

Lok Sabha; 9 December 2022

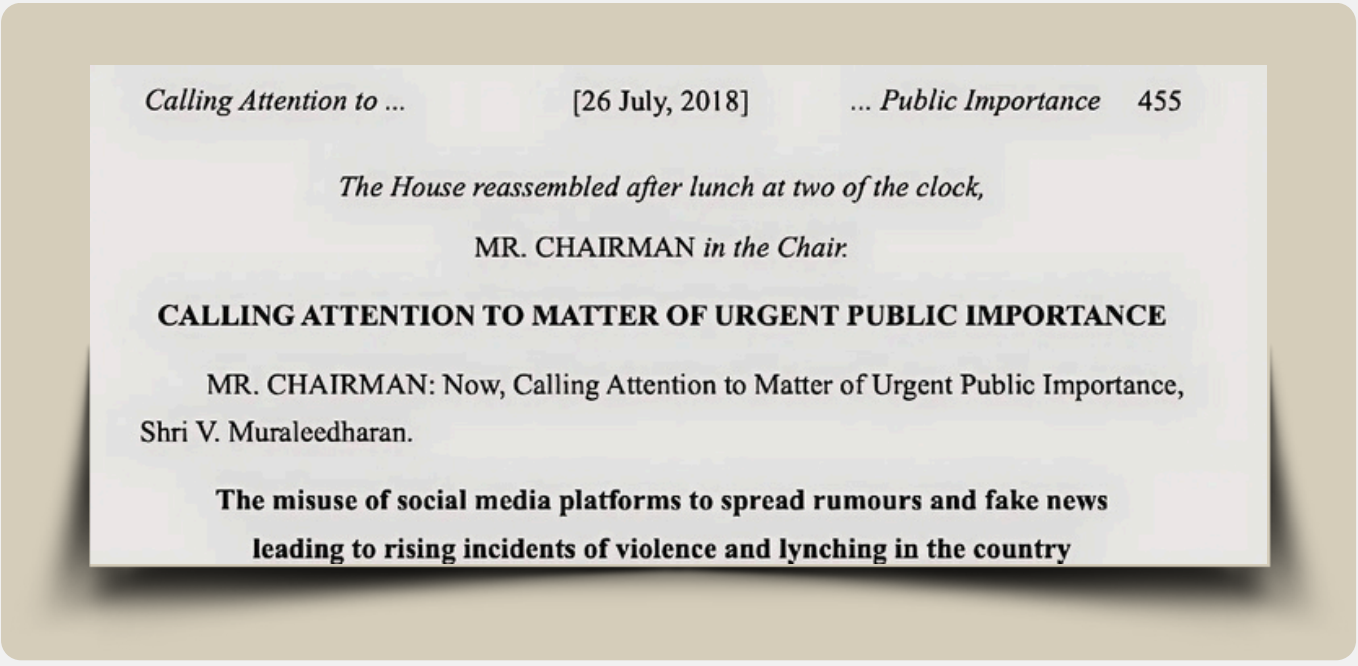
CALLING ATTENTION

Purpose

Members can direct a Minister's attention to urgent issues, prompting immediate statements or follow-up actions on matters like cybersecurity and digital safety.

Impact

This mechanism catalyses policy discussions, raises awareness, and drives the government's focus toward critical cybersecurity issues, leading to incremental improvements in strategies.[26]



Calling Attention to ... [26 July, 2018] *... Public Importance* 455

The House reassembled after lunch at two of the clock,

MR. CHAIRMAN *in the Chair.*

CALLING ATTENTION TO MATTER OF URGENT PUBLIC IMPORTANCE

MR. CHAIRMAN: Now, Calling Attention to Matter of Urgent Public Importance, Shri V. Muraleedharan.

The misuse of social media platforms to spread rumours and fake news leading to rising incidents of violence and lynching in the country

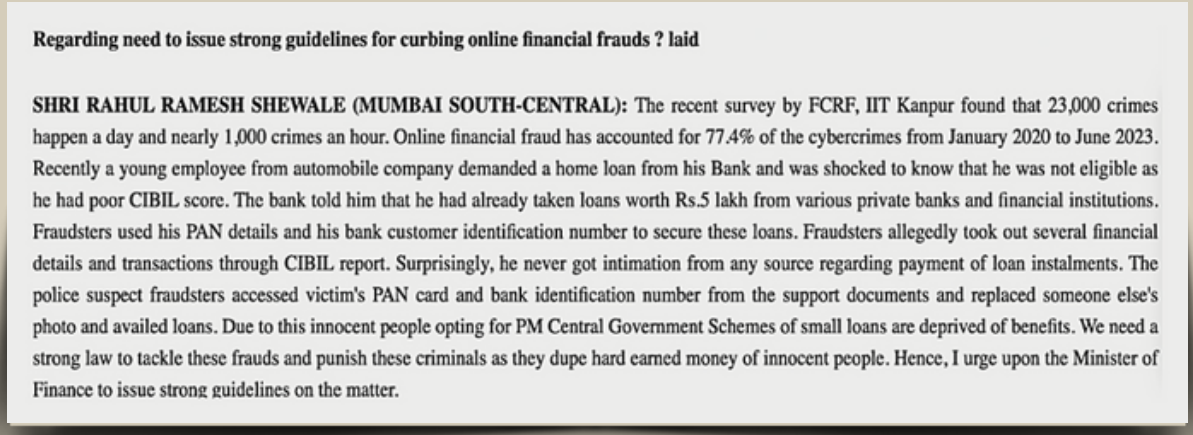
PRIVATE MEMBER RESOLUTION

Purpose

Members can use this mechanism to propose resolutions, formally request action or express opinions on key digital issues like access, privacy, or free speech.

Impact

These resolutions help bring critical digital rights issues into the public discourse, fostering scrutiny and driving legislative changes to protect citizens' online freedoms.[27]

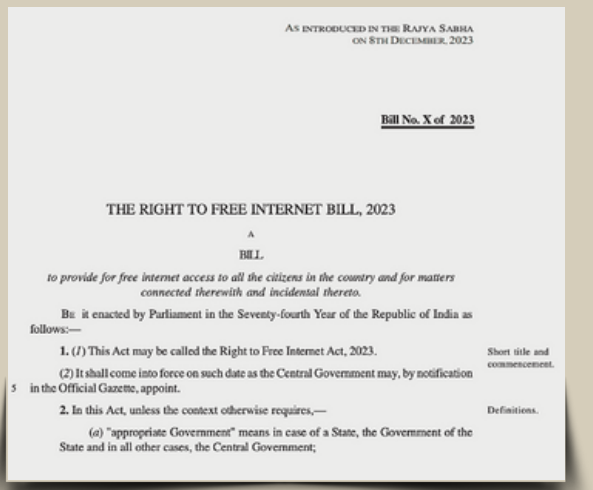


Regarding need to issue strong guidelines for curbing online financial frauds ? laid

SHRI RAHUL RAMESH SHEWALE (MUMBAI SOUTH-CENTRAL): The recent survey by FCRF, IIT Kanpur found that 23,000 crimes happen a day and nearly 1,000 crimes an hour. Online financial fraud has accounted for 77.4% of the cybercrimes from January 2020 to June 2023. Recently a young employee from automobile company demanded a home loan from his Bank and was shocked to know that he was not eligible as he had poor CIBIL score. The bank told him that he had already taken loans worth Rs.5 lakh from various private banks and financial institutions. Fraudsters used his PAN details and his bank customer identification number to secure these loans. Fraudsters allegedly took out several financial details and transactions through CIBIL report. Surprisingly, he never got intimation from any source regarding payment of loan instalments. The police suspect fraudsters accessed victim's PAN card and bank identification number from the support documents and replaced someone else's photo and availed loans. Due to this innocent people opting for PM Central Government Schemes of small loans are deprived of benefits. We need a strong law to tackle these frauds and punish these criminals as they dupe hard earned money of innocent people. Hence, I urge upon the Minister of Finance to issue strong guidelines on the matter.

Lok Sabha; 7 December 2023

PRIVATE MEMBERS' BILL



AS INTRODUCED IN THE RAJYA SABHA
ON 8TH DECEMBER, 2023

Bill No. X of 2023

THE RIGHT TO FREE INTERNET BILL, 2023

A

BILL

to provide for free internet access to all the citizens in the country and for matters connected therewith and incidental thereto.

BE it enacted by Parliament in the Seventy-fourth Year of the Republic of India as follows:—

1. (*1*) This Act may be called the Right to Free Internet Act, 2023. — Short title and commencement.

(*2*) It shall come into force on such date as the Central Government may, by notification in the Official Gazette, appoint.

2. In this Act, unless the context otherwise requires,— — Definitions.

(*a*) "appropriate Government" means in case of a State, the Government of the State and in all other cases, the Central Government;

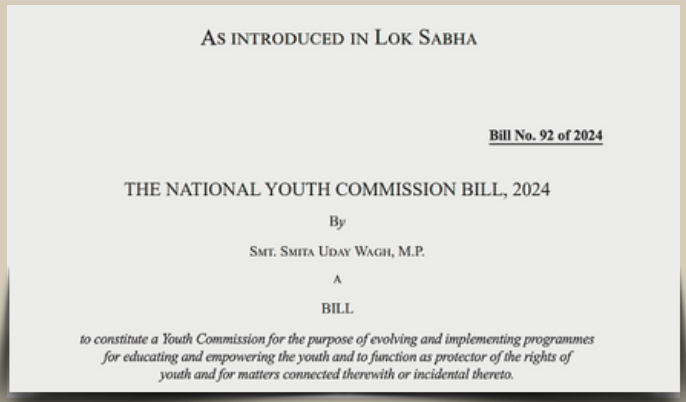
The Right to Free Internet Bill

Purpose

Members, who are not Ministers, can propose new laws to address emerging online safety issues, such as deepfakes and digital harassment, by focusing on the legal and regulatory frameworks needed to combat these threats.

Impact

These bills help shape legislative responses to digital harms, driving comprehensive measures to safeguard citizens and strengthen cybersecurity.[28,29]



AS INTRODUCED IN LOK SABHA

Bill No. 92 of 2024

THE NATIONAL YOUTH COMMISSION BILL, 2024

By

SMT. SMITA UDAY WAGH, M.P.

A

BILL

to constitute a Youth Commission for the purpose of evolving and implementing programmes for educating and empowering the youth and to function as protector of the rights of youth and for matters connected therewith or incidental thereto.

IDENTIFY
Identify a gap in existing digital safety legislation

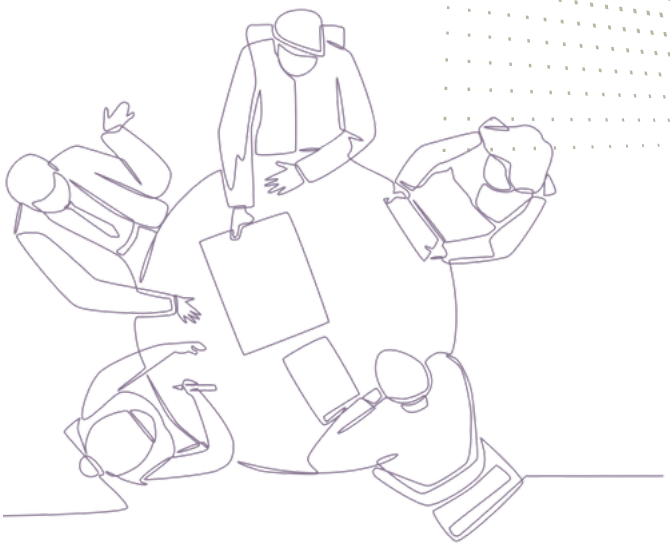
DRAFT
Research and draft the bill

SUPPORT
Seek support from fellow MPs

INTRODUCE
Introduce the bill in the House

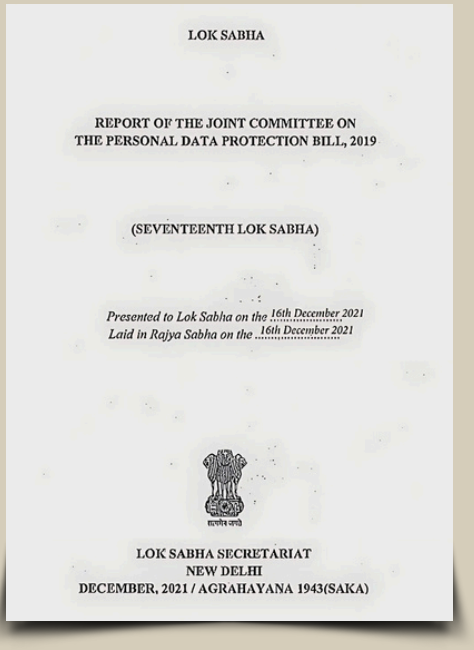
CHAMPION
Push for the bill's consideration and passage through speeches, debates, and community outreach.

HOW TO ENGAGE WITH PARLIAMENTARY COMMITTEES EFFECTIVELY ON ONLINE SAFETY



Purpose

As part of a Parliamentary Committee, Members can engage in discussions, participate in policy decisions, and contribute to strengthening laws.



LOK SABHA

REPORT OF THE JOINT COMMITTEE ON
THE PERSONAL DATA PROTECTION BILL, 2019

(SEVENTEENTH LOK SABHA)

Presented to Lok Sabha on the 16th December 2021
Laid in Rajya Sabha on the 16th December 2021

LOK SABHA SECRETARIAT
NEW DELHI
DECEMBER, 2021 / AGRAHAYANA 1943(SAKA)

The committee received 234 public submissions, conducted 78 detailed sittings over 184 hours, and facilitated consultations with ministries, industry experts, and regulatory bodies, including a study tour to Mumbai and Bengaluru for direct engagement with data centres and stakeholders, ensuring robust deliberations on data privacy and protection. [31]

Rajya Sabha sets up panel to study issues related to online pornographic content

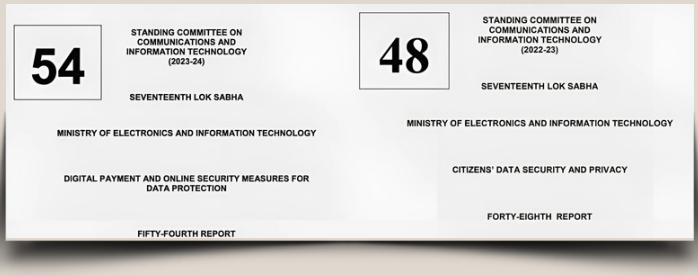
The group will be coordinated by Congress leader Jairam Ramesh.

Updated - December 05, 2019 07:14 pm IST - New Delhi

In December 2019, the Rajya Sabha Chairman announced the formation of a 14-member informal group to address issues related to pornographic content on the Internet and social media platforms. The informal group was changed into an ad-hoc committee, which aimed to engage with civil society groups and social media companies to gather insights and develop recommendations for legislative action.[30]

Impact

Active participation in committees provides access to expert insights and evidence-based recommendations, which help refine policies and drive legislative reforms.



54

STANDING COMMITTEE ON COMMUNICATIONS AND INFORMATION TECHNOLOGY (2023-24)

SEVENTEENTH LOK SABHA

MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

DIGITAL PAYMENT AND ONLINE SECURITY MEASURES FOR DATA PROTECTION

FIFTY-FOURTH REPORT

48

STANDING COMMITTEE ON COMMUNICATIONS AND INFORMATION TECHNOLOGY (2022-23)

SEVENTEENTH LOK SABHA

MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

CITIZENS' DATA SECURITY AND PRIVACY

FORTY-EIGHTH REPORT

During the 17th Lok Sabha, the Committee on IT released reports such as the Fifty-Fourth Report on Digital Payment and Online Security Measures for Data Protection and the Forty-Eighth Report on Citizens' Data Security and Privacy. These reports provided critical analysis and recommendations for strengthening data protection and enhancing cybersecurity measures. [32]

JOINING AND ENGAGING

Express interest in committees related to technology, women empowerment, or education.

Participate in hearings, discussions, and study tours.

Work with fellow members on bipartisan efforts.

WHAT TO DO AS A MEMBER

Recommend in-depth reviews of existing online safety frameworks.

Invite child safety NGOs, cybersecurity professionals, and tech specialists.

Scrutinise allocations for cybersecurity initiatives and digital literacy programs.

IV. Civic Engagement and Participation Mechanisms

Effective civic engagement is vital for promoting cyber safety at the grassroots level. Parliamentarians are in a strong position to drive these initiatives, both individually and collaboratively, ensuring robust protection for their constituents against online threats.

POLICY FEEDBACK FROM THE COMMUNITY

Business Standard

Over 70 eminent citizens write to MPs on Digi Personal Data Protection Bill

Over 70 eminent citizens, including former judges, officers have written to MPs to express their concern regarding the proposed DPDPB, 2022

In their letter, citizens highlighted issues with the public consultation process and urged MPs to ensure an extended consultation deadline and to advocate for a more accessible feedback mechanism, including offline submission options.[34]

Purpose

MPs can gather public feedback on proposed cyber safety laws to enhance transparency and engagement with diverse stakeholders, including industry experts, civil society, and vulnerable communities.

Impact

Using accessible online platforms, MPs can increase citizen participation in policymaking, ensuring laws are relevant and effective in addressing digital privacy and security concerns.

THE TIMES OF INDIA

Joint Parliamentary Committee on Waqf Bill to hold discussion in Guwahati today

ANI / Updated: Nov 9, 2024, 10:37 IST

Chaired by Shri Jagdambika Pal, the Committee held discussions as part of a study tour, covered five cities to examine the bill, and conducted meetings with various stakeholders, including representatives from various bodies and minority organisations.[35]

Manish Tewari
@ManishTewari

The arrest of @durov, the founder of Telegram, in France raises serious issues of liability qua digital platform owners for **user generated content.** Should @facebook, @X, @instagram be subject to the same legal architecture as Print & Broadcast Media?

If not, where does their liability for content on their platforms start and end? Can **safe harbour rules** be an open ended indemnity for anything & everything that gets posted on these platforms?

Manish Tewari
@ManishTewari

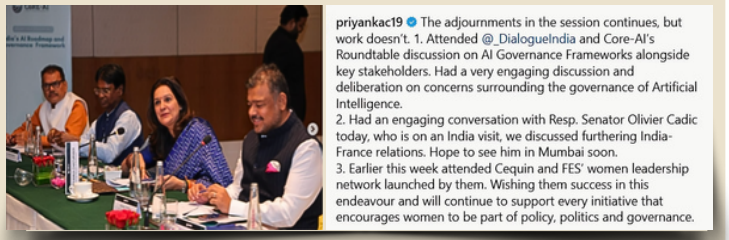
The news report pertaining to the sexual assault on an @airindia Crew Member in London is very disturbing. What makes it even more galling is that the Cabin Crew had been repeatedly complaining about the lack of security in the hotel in London, inadequate lighting and the dark spaces.

The @TataCompanies owned @Airindia chose to do nothing about it & therefore, deliberately put the Cabin Crew at risk.

Shri Manish Tewari regularly uses social media to engage with his constituents, address pressing issues, and foster meaningful public dialogue on governance, law, and societal responsibility.[36]

COMMUNITY ENGAGEMENT AND COLLABORATION WITH LOCAL INSTITUTIONS

Smt. Aparajita Sarangi actively participated in a breast cancer awareness community event and collaborated with local MLA Sidhant Mohapatra. She emphasised her commitment to promoting health awareness and engaging with the community on critical issues.[37]



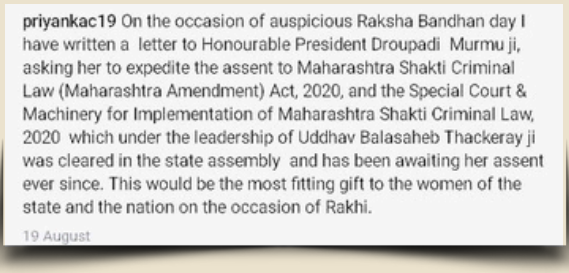
Smt. Priyanka Chaturvedi engaged with diverse stakeholders at local and international platforms, participating in discussions on AI governance, India-France relations, and women's leadership initiatives in policy and governance.[38]

Purpose

MPs have the opportunity to raise awareness about online threats and promote cyber safety by engaging with local communities and institutions through consultations, digital literacy initiatives, and partnerships with NGOs.

Impact

Effective community engagement allows MPs to identify specific concerns, drive awareness, and empower vulnerable groups (such as women, children, and the elderly) with knowledge.



Smt. Priyanka Chaturvedi wrote a letter to President Droupadi Murmu, urging expedited assent to the Maharashtra Shakti Criminal Law (Amendment) Act, 2020, and related provisions.[39]

Shri Praveen Khandelwal launched a series of public meetings called "Jan Chaupal" in June 2024, during which they recorded over 80 complaints from the constituents.[40]

MEMBER OF PARLIAMENT LOCAL AREA DEVELOPMENT SCHEME (MPLADS)

Purpose

MPs can leverage MPLADS funds to enhance cyber literacy and digital infrastructure in their constituencies. They can also collaborate with MLAs to improve local infrastructure and ensure the effective implementation of both central schemes and local development projects.

Impact

By leveraging MPLADS, MPs can empower constituents with digital skills, enhance online safety, and foster inclusive growth through improved connectivity and access to technology, particularly in underserved areas.

Recognising the learning gaps, MPs across six Indian states contributed 450 ICT-enabled devices (K-Yans) under MPLADS to government schools, including computers, projectors, and internet access.[41]

MPs conceptualised the CoW (Computers on Wheels) initiative based on the "ICU on Wheels" model, funded 100% of the capital costs for the first three CoWs, and coordinated with stakeholders for effective implementation.[42]


Bidar South constituency villages to get free Wi-Fi

MLA inaugurates internet connectivity in 13 villages

Updated - December 02, 2016 01:07 pm IST - Bidar:

In 2016, an MLA of Bidar in Karnataka launched an ambitious project through the MLALADs fund to provide free Wi-Fi connectivity in all villages of his constituency, aiming to make it a digital constituency.[43]

MPLADS for Comprehensive Online Safety in Your Community

- What if a campaign were launched in collaboration with NGOs to raise awareness about online threats like phishing and cyberbullying?
- How about organising training sessions with local schools and community centres?
- Could MPLADS-funded support centres for victims of cybercrime be established to provide assistance and resources?
- How can internet infrastructure be improved, such as expanding broadband access, while also offering digital upskilling programs in the community?

SAANSAD ADARSH GRAM YOJANA (SAGY)

Purpose

SAGY allows MPs to adopt and develop Gram Panchayats to create model villages focused on infrastructure and social development, such as education and health. MPs can use SAGY to integrate cyber safety initiatives, promoting digital literacy and safe online practices as part of rural development plans.

Impact

MPs can empower rural communities, create safer digital environments, and bridge the digital divide, serving as a model for integrating online safety into rural development efforts.

Karulai Adarsh Panchayath: Hi-Tech School for Online Classes

Model panchayat guideline for Karulai

MP adopts village under Centre's SAGY scheme

Updated - September 12, 2016 07:49 pm IST - MALAPPURAM:

Karulai Gram Panchayat in Malappuram District was selected by MP P.V. Abdul Wahab under the Saansad Adarsh Gram Yojana. To assist its tribal population, Pradhan Mantri Jan Dhan Yojna enrollment camps ensured social security coverage, while the National Digital Literacy Mission improved digital skills with support from NSS volunteers.[44]

Key efforts included financial literacy, skill training, cancer detection camps, and the "Samatha" literacy movement. During the COVID-19 pandemic, MPLAD funds of Rs. 7.13 lakhs were used to build four smart classrooms at Nedumkayam, benefiting 108 families in the Schedule Tribe colony.

COLLABORATION AND COORDINATION AMONG PARLIAMENTARIANS

Purpose

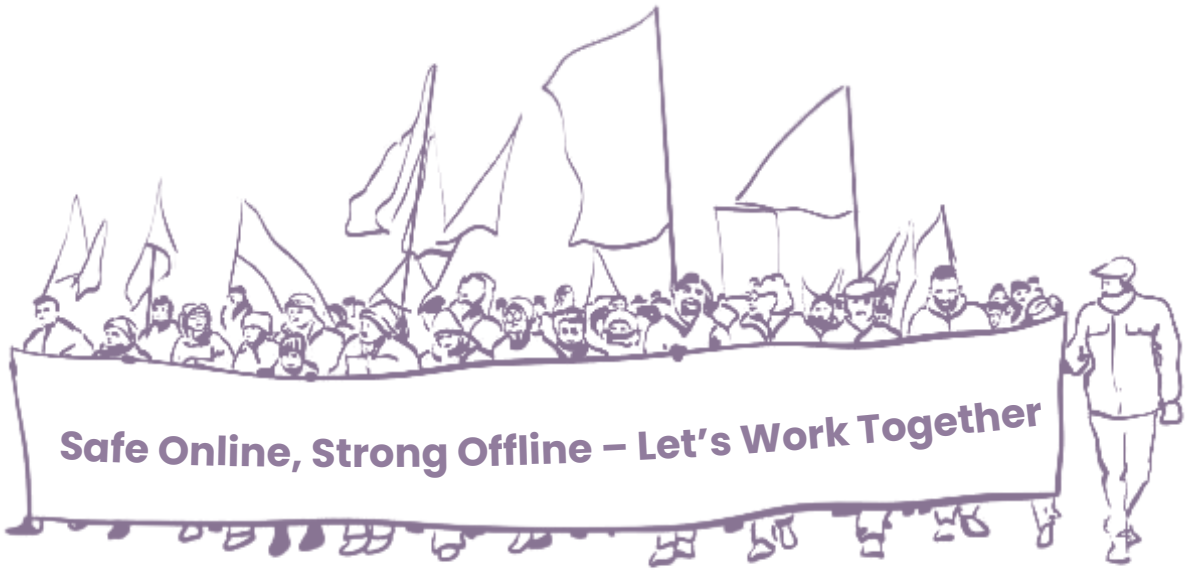
Collaboration among Parliamentarians is crucial to tackling the complex challenges of cyber safety. By working together across party lines, MPs can share insights, align priorities, and form unified responses to emerging digital threats.

Impact

This cooperative approach leads to more effective policy formulation, strengthened cybersecurity measures, and a collective effort that amplifies the impact of legislative actions to safeguard citizens in the digital space.

Shri Gaurav Gogoi - a three-time Member of Parliament and Member of the Standing Committee on Finance, engaged with The Public Policy Club at IIM Ahmedabad to share practical political experience and public policy expertise.[45]

Ms. Bansuri Swaraj attended the 5th edition of the NDTV Yuva Conclave, where she shared her views on women empowerment and Yuva Shakti with the attendees. [46]



HOW TO ENGAGE

Organise Cyber Safety Forums

Host bi-monthly or semi-annual forums with lawmakers, experts, and civil society to address emerging threats and propose solutions.

Facilitate Knowledge Sharing

Create an online repository of successful initiatives and organise workshops to share best practices across constituencies.

Coordinate Legislative Actions

Collaborate across party lines to draft and advocate for comprehensive cyber safety laws, focusing on shared priorities like child safety, data protection, and digital literacy.

Collaborating with the Private Sector

Purpose

MPs can partner with companies, especially those managing critical infrastructure, to promote community-based efforts and enhance digital infrastructure in their constituencies. Engaging through CSR initiatives can help develop relevant programs.

Impact

Through strategic partnerships, MPs can enhance local cybersecurity efforts, ensure the digital infrastructure needed for safe online environments, and drive sustainable solutions for their constituencies.

Project to revamp libraries at Kochi's Kalamassery

As a part of Minister P Rajeeve's 'Oppam' initiative, the project will have a budget allocation of Rs 1 crore from the CSR funds and will begin next month.

*The '**Grandhashalakalk Oppam Kalamassery**' project, led by Minister Shri P. Rajeev of the Kerala Assembly, exemplified collaboration with the private sector. Part of the 'Oppam' initiative, it renovated and digitised 25 libraries across Paravoor and Kanayannur taluks with a budget of Rs 1 crore, funded through CSR contributions from tech companies.*[47]

References

1. Press Information Bureau. (2024, July 25). Safeguarding India's Digital Landscape: Key Government's Initiatives to Enhance Cybersecurity Awareness. https://www.pib.gov.in/PressNoteDetails.aspx?NoteId=151959&ModuleId=3&reg=3&lang=1

2. Shukla, P. (2024, October 28). Indians lose over Rs 120 cr in digital arrest frauds; PM Modi cautions risk. Business Standard. https://www.business-standard.com/india-news/indians-lose-over-rs-120-cr-in-digital-arrest-frauds-pm-modi-cautions-risk-124102800276_1.html

3. WeProtect Global Alliance. (2023). Global Threat Assessment 2023: Assessing the scale and scope of child sexual abuse online. https://www.weprotect.org/global-threat-assessment-23/#full-report

4. National Centre for Missing & Exploited Children. (2023). CyberTipline 2022 Report. https://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata

5. National Crime Records Bureau. (2023). Crime in India 2022. https://www.ncrb.gov.in/uploads/nationalcrimerecordsbureau/custom/1701607577CrimeinIndia2022Book1.pdf

6. National Crime Records Bureau. (2023). Crime in India 2022. https://www.ncrb.gov.in/uploads/nationalcrimerecordsbureau/custom/1701607577CrimeinIndia2022Book1.pdf

7. Ministry of Home Affairs. (2024, January 4). Cyber Digest. https://i4c.mha.gov.in/cyber_digest/jan_2024/I4C%20Daily%20Digest-%2004.01.2024%20.pdf

8. (2024, January 30). Global data breach statistics: 2023 recap. Surfshark. https://surfshark.com/research/study/data-breach-recap-2023

9. Standing Committee on Communication and Information Technology. (2024, February 8). Digital Payment and Online Security Measures for Data Protection. https://sansad.in/getFile/lsscommittee/Communications%20and%20Information%20Technology/17_Communications_and_Information_Technology_54.pdf?source=loksabhadocs

10. Yadav, N. (2024, December 9). Dozens of schools get bomb threats in India's capital. BBC. https://www.bbc.com/news/articles/c140n7mrzeko

11. (2024, July 21). Global cyber attack surge 30% in Q2 2024, India hit hard. The Times of India. https://timesofindia.indiatimes.com/technology/tech-news/global-cyber-attacks-surge-30-in-q2-2024-india-hit-hard/articleshow/111899167.cms

12. Standing Committee on Communication and Information Technology. (2024, February 8). Digital Payment and Online Security Measures for Data Protection. https://sansad.in/getFile/lsscommittee/Communications%20and%20Information%20Technology/17_Communications_and_Information_Technology_54.pdf?source=loksabhadocs

References

13. (2023, November 13). From AIIMS Delhi to ICMR, data breaches haunt crores of Indians. The Economic Times. https://health.economictimes.indiatimes.com/news/health-it/from-aiims-delhi-to-icmr-data-breaches-haunt-crores-of-indians/105173060

14. The Digital Personal Data Protection Act, 2023 (Act 22 of 2023).

15. Ministry of Electronics and Information Technology. (2023, March 9). Proposed Digital India Act, 2023. https://www.meity.gov.in/writereaddata/files/DIA_Presentation%2009.03.2023%20Final.pdf

16. The Information Technology Act, 2000 (Act 21 of 2000).

17. Ministry of Electronics and Information Technology. National Cyber Security Policy, 2013.

18. Ministry of Electronics and Information Technology. National Policy on Information Technology, 2012.

19. Deb, S. (2024, December 2). What India's AI Safety Institute could do. The Hindu. https://www.thehindu.com/opinion/op-ed/what-indias-ai-safety-institute-could-do/article68935356.ece

20. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules. 2021.

21. Lok Sabha. (2022, December 7). Cyber Crime against Children. https://sansad.in/getFile/loksabhaquestions/annex/1710/AS16.pdf?source=pqals

22. Lok Sabha. (2024, July 31). Deepfake. https://sansad.in/getFile/loksabhaquestions/annex/182/AU1416_ZpirmY.pdf?source=pqals

23. Lok Sabha. (2024, February 6). Centres for Prevention of Cyber Crimes. https://sansad.in/getFile/loksabhaquestions/annex/1715/AU667.pdf?source=pqals

24. Lok Sabha. (2021, December 13). Demand to develop an appropriate education system for children in the country. https://sansad.in/ls/debates/view-debate?ls=17&session=7&dbslno=8432

25. Lok Sabha. https://sansad.in/ls

26. Rajya Sabha. https://sansad.in/rs

27. Lok Sabha. (2023, December 7). Regarding the need to issue strong guidelines for curbing online financial fraud. https://sansad.in/ls/debates/view-debate?ls=17&session=14&dbslno=12662

28. (2024, July 21). Govt clears consideration of private member's bill on free internet. The Print. https://theprint.in/india/govt-clears-consideration-of-private-members-bill-on-free-internet/2184165/

29. Lok Sabha. https://sansad.in/ls

30. (2019, December 5). Rajya Sabha sets up panel to study issues related to online pornographic content. The Hindu. https://www.thehindu.com/news/national/rajya-sabha-sets-up-panel-to-study-issues-related-to-online-pornographic-content/article30186850.ece

References

31. Lok Sabha. (2021, December 16). Report of the Joint Committee on The Personal Data Protection Bill, 2019. https://eparlib.nic.in/bitstream/123456789/835465/1/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf

32. Standing Committee on Communication and Information Technology. (2024, February 8). Digital Payment and Online Security Measures for Data Protection. https://sansad.in/getFile/lsscommittee/Communications%20and%20Information%20Technology/17_Communications_and_Information_Technology_54.pdf?source=loksabhadocs

33. Standing Committee on Communication and Information Technology. (2023, August 1). "Citizens" Data Security And Privacy" . https://eparlib.nic.in/handle/123456789/2505169?view_type=browse

34. (2022, December 16). Over 70 eminent citizens write to MPs on the Digi Personal Data Protection Bill. Business Standard. https://www.business-standard.com/article/economy-policy/over-70-eminent-citizens-write-to-mps-on-digi-personal-data-protection-bill-122121601262_1.html

35. (2024, November 9). Joint Parliamentary Committee on Waqf Bill to hold discussion in Guwahati today. Times of India. https://timesofindia.indiatimes.com/india/joint-parliamentary-committee-on-waqf-bill-to-hold-discussion-in-guwahati-today/amp_articleshow/115104715.cms

36. (2024, September 9). Manish Tewari. https://www.instagram.com/p/C_rIMOItyRJ/?hl=en&img_index=1

37. (2024, October 27). Aparajita Sarangi. https://www.instagram.com/p/DBnIuuOvO2h/?hl=en&img_index=1

38. (2024, November 30). Priyanka Chaturvedi. https://www.instagram.com/p/DC6eKvPoQKa/?hl=en&img_index=1

39. Priyanka Chaturvedi. (2024, August 23).https://www.instagram.com/p/C_AA8wkJtN7/?hl=en

40. (2024, June 12). Chandni Chowk MP Khandelwal launches 'jan chaupal'. The Hindustan Times. https://www.hindustantimes.com/cities/delhi-news/chandni-chowk-mp-khandelwal-launches-jan-chaupal-101718130455113.html

41. CII Foundation. (2014). Compendium of Successful Development Initiatives by Members of Parliament Under MPLAD Scheme. https://ciifoundation.in/document/MPLADSCompendium.pdf

42. CII Foundation. (2014). Compendium of Successful Development Initiatives by Members of Parliament Under MPLAD Scheme. https://ciifoundation.in/document/MPLADSCompendium.pdf

43. (2016, November 3). Bidar South constituency villages to get free Wifi. The Hindu. https://www.thehindu.com/news/national/karnataka/Bidar-South-constituency-villages-to-get-free-Wifi/article15948977.ece

44. (2016, September 12). Model panchayat guideline for Karulai. The Hindu. https://www.thehindu.com/news/national/kerala/model-panchayat-guideline-for-karulai/article8632388.ece/amp/

References

45. Gaurav Gogoi. (2024, December 5). https://www.instagram.com/pubpol_iima/p/DDKURxdgkI9/?hl=en

46. Bansuri Swaraj. (2024, September 19). https://www.instagram.com/p/DAGYxAxiNIa/?hl=en&img_index=1

47. (2024, October 22). Project to revamp libraries at Kochi's Kalamassery. The New Indian Express. https://www.newindianexpress.com/amp/story/cities/kochi/2024/Oct/22/project-to-revamp-libraries-at-kochis-kalamassery.

The Dialogue®
INFORM ENGAGE IDEATE

2024

Thank you!

Thank you for taking the time to read this handbook. If you have any questions or would like to discuss our findings further, please don't hesitate to reach out to us.

thedialogue.co

LinkedIn | The Dialogue

Twitter | The Dialogue

Whatsapp | The Dialogue

Instagram | The Dialogue