THE CENTRE FOR internet & society

# LEGAL ADVOCACY MANUAL:

## A primer on the jurisprudence of digital rights in India

By (in alphabetical order) Radhika, Shruti Trikanad and Torsha Sarkar

**DESIGN**
Aparna Chivukula

*This work was supported by a research grant from the East-West Management Institute (EWMI). All errors remain the authors' own.*

# LEGAL ADVOCACY MANUAL:

## A primer on the jurisprudence of digital rights in India

By (in alphabetical order) Radhika, Shruti Trikanad and Torsha Sarkar

THE CENTRE FOR internet & society

# Contents

# Content Takedown

Content takedown laws empower the government to request internet "intermediaries" to censor content that violates the local law of the country. Intermediaries are a particular class of entity defined under the Information Technology (IT) Act of 2000, and encompass a variety of online gatekeepers, like payment gateways, social media platforms, search engines and so on.

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, ["IL Rules 2021"], which were enacted under the IT Act, introduces two subcategories of "intermediaries" which more varied content takedown requirements apply to. Therefore by the operation of the IT Act and the IL Rules 2021, there are currently three different categories online entities to which content takedown requirements apply to:

a) '**Intermediary**': As per the definition in the IT Act, an intermediary "*means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web hosting service providers, search engines, online payment sites, online-auction sites, online marketplaces and cyber cafes.*"[1]

b) '**Social Media Intermediary**' (**SMI**): These are defined in the 2021 rules, as intermediaries which "*primarily or solely enables online interaction between two or more users and allows them to create, upload, share, disseminate, modify or access information using its services.*"[2]

c) '**Significant Social Media Intermediary**' (**SSMI**): Also defined within the 2021 rules, a SSMI is a social media intermediary with a certain user threshold, as would be notified by the Central Government.[3] As of the time of writing this, the government has notified this threshold to be 50 lakhs, or 5 million registered users.[4]

This attempt at classifying the intermediaries is a step towards the right direction. In the previous renditions of these rules, including the draft version floated in 2018, intermediaries were generally treated as a single, monolithic entity, much to the concern of civil society organisations and private companies, since the resulting regulation then became one-size-

1 Section 2(w), IT Act

2 IL Rules 2021, Rule 2(w).

3 IL Rules 2021, Rule 2(v).

4 http://egazette.nic.in/WriteReadData/2021/225497.pdf

fits-all, erasing much of the nuances present in the internet ecosystem.[5] However, concerns regarding the definition of these three terms remain. We discuss these in a little more detail below.

## 'Intermediary'

Significant portions of Rule 3 and Rule 4 of the IL Rules 2021 comprise content takedown requirements that intermediaries and SMIs must adhere to, and includes, for instance, publication of Terms and Conditions (ToC) listing certain kinds of content that the users would be prohibited from posting, responding to government notices on censorship ("takedown notices") within a specific time period, and so on.

The issue here, however, is that a majority of these requirements still continue to apply to 'intermediaries' as a whole. The definition of 'intermediaries' as it currently stands, encompasses a vast plethora of entities, including internet service providers, cyber cafes, and online payment services. While content takedown requirements make sense for entities like Facebook and Twitter — whose services concern user content (and which would, arguably fulfil the criteria of a SMI) — to be able to comply with these content takedown requirements, it would be absurd to expect, for instance, cyber cafes, or internet exchange providers or Open source groups running decentralised messaging platforms such as Matrix, to comply with similar requirements and follow similar legal routes. Enforcing such a requirement would contribute to creation of further regulatory uncertainty amongst these services.

## 'Social Media Intermediary' (SMI)

As indicated above, a SMI is defined as any intermediary who enables online interaction between two or more 'users' and allows them to share, upload, modify 'information', etc. Taken together, the ambit of a SMI becomes exceptionally broad, and would bring about nearly every entity engaged with facilitating any sort of 'interaction' between two or more users within its scope. Further, this conceptualization is absolute in nature and without any exceptions for either platforms operating without a profit motive (including online encyclopaedias like Wikipedia), or for entities solely facilitating private communication between users.

In addition, given the broad definition, a substantive number of entities that are cited as illustrations of an 'intermediary' within the meaning of Section 2(w) of the IT Act, including, "telecom service providers, network service providers, internet service providers, web hosting service providers, search engines, online payment sites, online-auction sites, online marketplaces and cyber cafes" would probably still fulfil the criteria of a SMI. In that case, this attempt at classification between an intermediary and a SMI becomes redundant.

5 https://cis-india.org/internet-governance/blog/torsha-sarkar-november-30-2019-a-deep-dive-into-content-takedown-timeframes

### 'Significant Social Media Intermediary' (SSMI)

Finally, a SSMI is currently defined as a SMI with fifty lakh, or five million registered users in India. As per the operation of the rules in toto, SSMIs seem to bear an additional level of compliance around content takedown requirements, including a higher level of transparency and accountability towards its users.

This is a step towards the right direction, and would bring these entities within adherence of Principle 14 of the UN Guiding Principles on Business and Human Rights, which emphasise that the "*means through which a business enterprise meets its responsibility to respect human rights will be proportional to, among other factors, its size*."[6]

However, the government notification to this effect is unclear and inadequate in terms of how this user threshold would be calculated. The NetzDG in Germany, for instance, which is supposed to be applicable to intermediaries with 2 million registered users, also ran into a similar problem, since it had not clarified whether the user-count would be calculated on the basis of an active user-base, or an average value calculated over time. In a similar vein, the current framework for the calculation of user thresholds for SSMIs operating in India, is currently clouded in ambiguity.

Finally, the specific details of the user threshold to qualify as a SSMI are also concerning. The current threshold is set at 50 lakh, that translates to 5 million registered users. In comparison, the NetzDG has 2 million as its threshold in a country where 88% of the population[7] (out of a total of 83.1 million[8]) or 73 million people use the internet. The threshold set by the German Government is, thus, 2.7% of the digital population. Whereas, in India, with an internet-using population of approximately 776 million[9], the threshold is 5 million — which is less than 0.007% of the Indian digital population. Setting such a low threshold, therefore, might create additional hurdles for smaller social media intermediaries and in fact disincentivize growth in smaller SMIs.

## Background

An online intermediary's relationship to content hosted on its platforms by third-parties, has evolved significantly over the past two decades, and this evolution has been reflected in legislative efforts around the world. The late 1990s and the early 2000s were characterised by a *laissez-faire* approach to the regulation of intermediary liability, which meant important jurisdictions enacted legislations that accorded large amounts of immunity to intermediaries for unlawful content posted by their users.

6 https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf

7 https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=DE

8 https://data.worldbank.org/indicator/SP.POP.TOTL?locations=DE

9 https://www.trai.gov.in/sites/default/files/QPIR_21012021_0.pdf

For instance in the European Union (EU), the E-commerce Directive, which was enacted in 2000, stated that an information society provider (an entity similar to an intermediary) would not be liable for information stored, provided that the information society provider[10] did not not have 'actual knowledge' of illegal activity, and on the receipt of illegal activity, expeditiously removed access to such information.[11]

Similarly, in the United States of America (USA), section 230 of the Communications Decency Act (CDA) granted strong immunity to intermediaries against unlawful speech posted by their users, stating that: "*No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider*."

Throughout the early 2000s, the Indian government arrived at a similar legislative stance.

## *Avneesh Bajaj v State*

In 2004, a viral video clip of two minors involved in a sexual act was found to be sold on Bazee.com, an e-commerce website that was owned by eBay. Following media attention, the CEO of Bazee.com, Avnish Bajaj was arrested[12] and charged with making available for sale and publication of an obscene product. In *Avneesh Bajaj v State*, which came up in front of the Delhi High Court in 2008, he petitioned the court to quash the criminal proceedings against him. However, the Delhi High Court only quashed specific charges against him, finding that there was a prima facie case made against him under provisions of the IT Act.

Following this, the IT Act was amended in 2008. In particular, section 79, which had earlier contained a proto-version of intermediary liability protection, was amended to include a more detailed regulatory framework. We unpack the elements of the provision in the subsequent sections. In 2011, the Indian government further passed the Information Technology (Intermediaries guidelines) Rules ["IL Rules 2011"].

Under the framework erected by section 79 and the IL Rules 2011, an intermediary would be exempted from liability for content posted by its users (that is, entitled to a 'safe harbour' protection). As per Rule 3(4), this exemption would only apply when the intermediary took down any offending content within 36 hours of deriving 'actual knowledge' about the existence of such content. The IL Rules further provided that an intermediary would be construed to have 'actual knowledge' of offending content, once it has obtained such knowledge itself, or when it has been brought to the intermediary's attention by *an affected person* in writing.

10 https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32000L0031

11 The E-commerce Directive, Article 14

12 https://web.archive.org/web/20161011234432/http://expressindia.indianexpress.com/news/fullstory.php?newsid=39787

The impact of this rule was that the intermediary would be legally obligated to respond to content removal requests (*hereinafter* 'takedown notices') from numerous third parties, and would have to act on them within a short time-frame, with the subtext being that in case the intermediary was found in non-compliance, it would lose its legal immunity, and be (potentially) criminally liable for content posted by its users. The implication of this, as was empirically investigated, was that intermediaries were over-complying with flawed takedown notices, and censoring legitimate content[13], at the apprehension of legal sanctions.

Additionally, Rule 3(2) listed down further due diligence obligations that the intermediary was obligated to follow. This included the obligation to display rules and regulations rules and regulations that inform users that they were prohibited from posting a variety of unlawful information, which included information that was "*grossly harmful, harassing, blasphemous defamatory, obscene, pornographic, paedophilic, libellous, invasive of another's privacy* [...]".

Apart from this, the amendment to the IT Act also introduced section 69A, which empowered the government to issue blocking orders to intermediaries under grounds mentioned under section 69A. Similar to section 79, section 69A had allied rules, titled the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 ["the blocking rules 2009"].

The blocking rules introduced a detailed procedure via which the government was to issue takedown notices to the intermediary. This procedure has been criticised for being heavily executive-driven, with there being little judicial oversight over the process of determining what content gets taken down.[14] Additionally, the rules also introduced a confidentiality requirement in the procedure for censoring content. This has meant that the government is not obligated to be accountable to the public at large about whether the safeguards encoded in the blocking rules are being fulfilled or not. This rule has also allowed the government to circumvent RTI requests about the nature of content blocked.[15]

## *Shreya Singhal v Union of India*

In 2015, in the case of *Shreya Singhal v Union of India*, the constitutional validity of both section 79 and section 69A was called into question in front of the Supreme Court of India. This is considered a landmark judgement in the Intermediary Liability landscape in the country.

**Regarding section 69A**: The petitioners challenged the constitutional validity of section 69A and the blocking rules on the following grounds:

a) As per the procedure under the rules, there was no provision to ensure that the

13 https://cis-india.org/internet-governance/chilling-effects-on-free-expression-on-internet

14 https://theleaflet.in/content-takedown-and-users-rights/

15 https://sflc.in/rti-meity-provides-details-blocked-websitesurls

originator of the information — i.e., the person whose content is impugned — to get a hearing before a decision to block their content is arrived at.

b) The blocking rules do not have sufficient procedural safeguards. For contrast, the petitioners cited section 95 and section 96 of the Code of Criminal Procedure (CrPC), which allows the State government to ban books, and allows people to challenge these actions in a court.

c) Finally, the petitioners stated that the confidentiality requirement under the blocking rules was unconstitutional, since it impacted the fundamental rights of the petitioners.

The court however, did not find sufficient merit in these arguments. Specifically, the court found that section 69A was narrowly drawn and had several safeguards, which were: a) a blocking order under the provision could only be issued when the Central Government was satisfied that it was necessary to do so, b) the grounds under which such a blocking order could be issued were related to Article 19(2) of the Indian Constitution, which laid down reasonable restrictions to the right to speech and expression, and c) the reasons for issuing a blocking order were to be written down, to ensure that such orders could be challenged in a court. As per these reasons, the court found that section 69A was constitutionally valid.

**Regarding section 79**: The petitioners challenged the constitutional validity of section 79 and the IL Rules 2011 on the following grounds:

a) The ambit of Rule 3(2) was vague and ambiguous.

b) The takedown process under the legal framework made the intermediary exercise their own judgement upon receiving 'actual knowledge' of unlawful information.

c) The petitioners also pointed out that the definition of the term 'unlawful' as per the legal framework, went beyond the specified subjects delineated under Article 19(2).

Unlike section 69A, for the constitutional challenge to section 79, the court took stock of the petitioner's arguments. The court found that section 79 was an exemption provision, which meant, it laid down the conditions for the intermediary to seek the exemption from liability. Having said that, the court also found that section 79 was closely related to provisions which provide for offences, including under section 69A. However, according to the court, under section 69A, blocking could only take place by a reasoned order, and only after the procedural safeguards under the legal framework were met. Under the framework of section 69A therefore, there was no provision for intermediaries to apply their own mind regarding whether information should be blocked.

Accordingly, the court read down the ambit section 79, with two caveats. *First*, an intermediary will be presumed to have 'actual knowledge' only when a court order or a government notification has been passed, requiring the intermediary to take down content. *Second*, the court order or the government notification must strictly conform to the subject matters laid

down in Article 19(2), which means that intermediaries would not be legally obligated to act on any takedown order that requires them to take down content on grounds beyond the reasonable restrictions on the right to freedom of speech and expression.

With these two caveats, the court refrained from striking down section 79 from the IT Act.

## *Challenges to blocking Free Software applications - Briar and Element*

It was widely reported during the first week of May that 14 applications had been blocked in India. Section 69A of the Information Technology Act, 2000 was invoked to restrict these applications, citing allegations of being utilised for communication between malicious actors in the Jammu and Kashmir region.[16] Two popular FOSS programs that are used on a daily basis by software engineers, technicians, innovators, and entrepreneurs—"Element" and "Briar"—were included in the list of applications that were prohibited. There are two petitions challenging these blocks in Delhi High Court and Kerala High Court.[17, 18]

### *Sublime Software v. Union of India*

A petition was filed by the Founder of Briar application in the High Court of Delhi. The order for blocking the app was not made public even to the petitioner of the case in question; neither was an intimation or any kind of notice. Per the last hearing, a notice has been issued by the court in the matter.

### *Praveen Arimbrathodiyil V. Union of India*

Free and open-source software (FOSS) developer Praveen Arimbrathodiyil, a volunteer member of the Free Software Community of India (FSMI), filed a writ petition under Article 226 of the Indian Constitution, challenging the Central Government's order under Section 69A of the Information Technology Act, 2000, prohibiting the widely used FOSS messaging platforms "Element" and "Briar." Additionally, he challenged Rule 16 of The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 (also known as the "Blocking Rules, 2009"), deeming them in violation of Articles 14, 19, and 21 of the Indian Constitution.

16 https://scroll.in/latest/1048331/centre-blocks-14-messaging-apps-allegedly-used-by-terror-groups-in-j-k-say-reports

17 https://sflc.in/sflc-in-assists-in-legal-challenge-to-the-blocking-of-foss-messaging-platform-briar-before-delhi-high-court/

18 https://sflc.in/sflc-in-assists-in-challenge-to-blocking-of-foss-apps-element-and-briar-before-kerala-high-court/

# Current law and jurisprudence

In the following sections, we go over some current issues of law concerning the provisions already discussed.

## Section 69A and accountability

Despite *Shreya Singhal*'s affirmation about the constitutionality of section 69A, counsel for the petitioners' had subsequently pointed out that there has been no recorded instance of pre-decisional hearing being granted to the originator of the information.[19] This has meant that the safeguards, so espoused by the Supreme Court, have never been actually implemented.

On top of that, as indicated earlier section 69A has an embedded confidentiality requirement, which has made it difficult to seek information around the government's actions under the provision. This adds an additional hurdle in ascertaining whether the safeguards and procedures listed under the blocking rules are truly followed.

**The case of Dowrycalculator.com**: In 2018, Tanul Thakur, the creator of the website dowrycalculator.com, found out that his website had been blocked.[20] Dowrycalculator.com was set up to satirise the regressive custom of dowry.[21] Nevertheless, the government had blocked the website, without giving Thakur, who was the originator within the meaning of the blocking rules, an opportunity of hearing. He subsequently filed multiple RTI requests, in hopes of obtaining the original blocking order that had led to the unavailability of the website, and each of these were rejected, with the government only giving evasive answers each time, and citing Rule 16 of the blocking rules.

At the end of 2019, Thakur approached the Delhi High Court, challenging the arbitrary blocking of his website. His petition requested the court to direct the unblocking of the website, and to declare that Rule 16 of the blocking rules was unconstitutional.

After significant back and forth, in May 2022, the Delhi High Court finally asked the government to supply Thakur with the original blocking order, and allow him a chance to defend the website in front of the committee constituted under the blocking rules.

This was an important decision by the Court, since in the past content creators or intermediaries have not usually been given a chance to respond to blocking requests.[22] Rule 16 has further enabled the government to not provide the original blocking order to the person whose content was taken down.

19 https://indianexpress.com/article/opinion/columns/but-what-about-section-69a/

20 https://internetfreedom.in/delhi-hc-issues-notice-to-the-government-for-blocking-satirical-dowry-calculator-website/

21 id

22 https://cyberbrics.info/content-takedown-and-users-rights/

Therefore, the Delhi High Court's order, directing the government to supply Thakur with the original copy of the blocking order, as well as allowing him to appear before the committee, was an important step towards more transparency in the content takedown process. It can be hoped that the trickle-down effect of this direction would benefit other content creators who have found their content arbitrarily blocked.

Finally, in lieu of the persisting problems around section 69A, in July 2022, Twitter India challenged the Indian government in the Karnataka High Court, over the government's recent orders to takedown content from its platform.[23] This lawsuit stood as the first and only lawsuit from an online platform, resisting the government's exercise of power under section 69A. As such, this is a pivotal moment in the history of content takedown in India.

The Karnataka High Court in June dismissed Twitter's challenge to the blocking rules issued by MEITY under Section 69A of the IT Act. Moreover a fine of 50 lakh was imposed on the corporation. The court found the orders issued by the ministry in compliance with the directions in the Shreya Singhal Judgement. Twitter inc (now X corp) has filed an appeal against this order.[24]

## Competent authorities

*Shreya Singhal* affixed that under section 79 of the IT Act, an intermediary would only be legally liable to act on takedown requests only on receipt of valid notices from competent authorities, which would be the court or the government.

In 2021, the IL Rules 2011 underwent an amendment, and the government passed the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ["IT Rules 2021"]. The IT Rules 2021 superseded the previous rendition of these rules, and set out the current legal framework for intermediary liability in India.

Rule 3(1)(d) of the IT Rules 2021 codifies the precedence laid down by Shreya Singhal, by stating that: "*an intermediary, on whose computer resource the information is stored, hosted or published, upon receiving actual knowledge in the form of an order by a court of competent jurisdiction or on being notified by the Appropriate Government or its agency*".

However, Rule 3(2)(b) of the IT Rules 2021 introduces additional content takedown obligations on intermediaries. This rule obligates intermediaries, on receipt of complaint from an individual or '*any person on their behalf*', to remove content that depicts private sexual matters of an individual or artificially morphed images of such an individual.

This is a notable exception to the precedence of *Shreya Singhal*, since the intermediary is being made legally liable to takedown requests from individuals. However, in this instance,

23 https://thediplomat.com/2022/07/twitter-files-lawsuit-against-indian-government-in-court/

24 https://www.livelaw.in/high-court/karnataka-high-court/karnataka-high-court-twitter-appeal-account-blocking-section-69a-it-act-234180

a case can be made that such an exception might be required, given that the scope of the content that is required to be removed is sensitive and urgent.

Rule 3(2)(b) aims to curb the online, non-consensual dissemination of intimate imagery (NCII). Often dubbed as 'revenge porn', this practice is often carried out with the purpose of "shaming, stigmatizing or harming the victim."[25] A report by IT for Change on women students in Tamil Nadu found that one of the most concerning forms of technology-mediated violence was the sharing of morphed images and the subsequent blackmailing by their use.[26]

In light of that, the framework of Rule 3(2)(b) might be justified, since an intermediary has the obligation to respect their user's privacy, dignity and autonomy, and can be asked to rapidly respond to the dissemination and distribution of NCII.[27]

However, the language of the provision does not consider 'consent' to be an important element, for an intermediary's liability to trigger. Consent is an important aspect of NCII, since many individuals, including those from marginalised communities, continue to consensually share photos and other visual materials that attempt to define their sexualities and identities. Additionally, the authorization to send a takedown notice under this provision is extended to not only the person whose imagery is being circulated, but to '*any person on [their] behalf*'. This is an exceptionally broad scope, and could be misused to censor speech online, especially speech that is originating from marginalised communities.[28]

## Automated content takedowns

Automated content takedowns are another contentious issue in the jurisprudence of content takedowns, partly because this is a relatively novel area of development. Nevertheless, in the past decade or so, Indian courts have had some chance to examine an online intermediary's obligation to deploy automated technologies and tools to filter, monitor and/or block content that is deemed to be 'unlawful'.

### *Sabu Mathew George v Union of India*

In 2008, Sabu Mathew George, an activist, filed a writ petition in the Supreme Court, requesting the court to ban advertisements relating to pre-natal sex determination from Google, Yahoo and Microsoft's search engines. As per the petitioner, the advertisements were violative of section 22 of the Pre-Natal Diagnostic Techniques (Regulation and Prevention of Misuse Act), 1994 ["the PNDT Act"].

Between 2014-15, the Supreme Court directed the respondent search engines to block such

25 https://undocs.org/pdf?symbol=en/A/HRC/38/47

26 https://itforchange.net/e-vaw/wp-content/uploads/2018/01/Dr_Radha.pdf

27 https://cis-india.org/internet-governance/legality-constitutionality-il-rules-digital-media-2021

28 https://cis-india.org/internet-governance/legality-constitutionality-il-rules-digital-media-2021

advertisements. Subsequently, on 19 September 2016, the Court ordered these search engines to develop a "*technique so that the moment any advertisement or search is introduced into the system, that will not be projected or seen by adopting the method of auto-block*."

The court termed this direction as the "*doctrine of auto-block*", and opined that this would ensure that no one would be able to access content that was illegal as per the PNDT Act. The court further ordered that alongside this doctrine, the search engines would also be expected to block the auto-completion of the search query. To achieve the outcomes described in these techniques, the court compiled a list of about 40 words for which auto-completion and results would be required to be blocked, and users who searched for these words would be shown a warning. Finally, the court directed the search engines to establish an in-house procedure to proactively filter content. In a follow-up order, passed on 16 November 2016, the Supreme Court directed the establishment of a 'nodal agency' that would be providing these search engines with the list of websites to block.

On 16 February 2017, the Court heard proceedings on the case again, wherein the Solicitor General, appearing for the Central Government, stated that a nodal agency had been constituted and individuals would be able to bring the existence of offending content to its notice. The Supreme Court directed the search engines to form an in-house expert committee that will further delete content from their platforms on their own interpretation of Section 22 of the PNDT Act. In case of any conflict, the committees would approach the nodal agency, and the latter's response would be constituted as the final decision in the matter. The case was finally disposed of on 13 December 2017.

By expecting intermediaries to proactively remove illegal content even without a takedown notice issued either by the court or by a government agency, the judgement in *Sabu Mathew George* directly contravened the precedent laid down in *Shreya Singhal* (see: Competent Authorities)[29]. Additionally, the technology suggested by the court, of auto-blocking search results based on a list of keywords, is flawed. In the history of content moderation, keyword blocking has been found to suffer from the 'Scunthorpe problem', where inadequate training of the technology has led to legitimate speech being removed or blocked. The origin of this problem can be traced back to 1996, where an AOL user was unable to upload the name of his hometown, Scunthorpe, on the platform, because AOL's keyword filter detected a string of letters within the word that was previously flagged to be obscene.[30]

In such light, without contextual clues around the keywords that are meant to be blocked, there is potential for the technology to even block educational or medical content, simply because they contain one or more of the prohibited words.[31] The court did not seem to

29 https://internetfreedom.in/statement-of-concern-on-the-sabu-mathew-george-case-dont-auto-block-online-expression/

30 http://catless.ncl.ac.uk/Risks/18.07.html#subj3

31 https://internetfreedom.in/statement-of-concern-on-the-sabu-mathew-george-case-dont-auto-block-online-expression/

prescribe any safeguards to ensure that this does not happen, and as such, the judgement could be made out to have a concerning impact on the exercise of freedom of speech and expression online.

### *In re: Prajwala*

In 2015, Prajwala, a NGO that works on eradicating sex trafficking, sent a letter to the Supreme Court, raising concerns about videos of sexual violence being available over the internet. The court took *suo motu* cognizance of the matter, and impleaded Google, Facebook, WhatsApp, Yahoo and Microsoft, as well as the Government of India, as respondents in the petition. After hearing the petitioner, early in 2017, the Court constituted a committee to assist and advise the court on the feasibility of ensuring that these videos were not available for circulation.

On 23 October 2017, the court heard the recommendations of the committee. The relevant recommendations were as follows:

> a) The Government of India may work with the represented companies and civil society organisations to suggest expansion of a list of keywords related to child sexual abuse material (CSAM). Any user opting to search using these keywords would be shown a warning or a public service message. The committee also recommended that these keywords may be gradually expanded to other Indian languages where applicable.
>
> b) The government of India could work with the impleaded companies and civil society organisations to suggest a list of keywords related to videos of sexual violence. Users who search using these keywords would be shown a similar warning or a public service message.

While the committee briefly discussed the possibility of incorporating artificial intelligence tools to assist in the process of removing CSAM or content of sexual violence, the committee did not directly recommend the adoption of these tools. Instead, it recommended that these technologies should be developed with greater collaborative work among stakeholders and suitable research must be initiated before further development of technologies for identifying CSAM or videos of sexual violence.

The only concrete recommendation that the committee made was to establish a hash-matching system for CSAM. Hash-matching is a commonly adopted version of using automated technologies to filter, monitor and block content. In this process, a piece of content is represented as a hash, which would essentially be a numerical representation of the file and comparatively smaller in size than the original file.[32] When a piece of content is tagged as 'illegal', it is tagged with a hash and entered into a database. Any future uploads of the same

32 https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/58d058712994ca536bbfa47a/1490049138881/FilteringPaperWebsite.pdf

content is then matched against this database, and automatically flagged.[33] The committee recommended that the impleaded companies in the case, should voluntarily collaborate with the National Centre for Missing and Exploited Children (NCMEC), to establish a shared database of CSAM video hashes, similar to hashes of CSAM image that are already being used by the industry.

Throughout the rest of 2017-18, the court heard the petitioners and the respondents several times, towards the implementation of these recommendations. On a hearing dated 28 November 2018, the government indicated that there were certain actions that the impleaded intermediaries were required to take, including setting up "*proactive monitoring tools for auto deletion of unlawful content by deploying Artificial intelligence based tools*". Following this, on a hearing dated 11 December 2018, the court directed the government to frame necessary guidelines and implement them, to eliminate CSAM and content related to sexual violence. With this, the court disposed of the petition.

There are two things of interest here. *Firstly*, the court in *Prajwala* does not direct intermediaries to adopt any technological means to filter, monitor or block illegal content. Rather, it seems to leave this decision up to the government and/or the constituted committee. *Secondly*, while the committee, in its recommendations, deliberated on a specific form of technological tool that intermediaries could adopt, the government's submission on the hearing dated 28 November 2018, is less specific, mentioning only the concept of "*proactive monitoring tools*".

## Proactive monitoring under the IL Rules 2021

The Intermediary Guidelines, 2021 offer a framework for regulating the content of online publications, including news publishers, curators of audio-visual content, and social media intermediaries. These guidelines supersede the old Information Technology (Intermediaries Guidelines) Rules, 2011. The Intermediary Guidelines, 2021 aim to establish a comprehensive framework for regulating information housed on the internet and improving transparency between platforms and users, ultimately leading to a greater degree of accountability. The Rules set forth the requirements for social media intermediaries in terms of graded due diligence, as well as an internal grievance redressal system, an online curated content code of ethics, self-regulation for publishers, and an executive monitoring mechanism. These rules have given powers to the Ministry of Information and Broadcasting (MIB) to take down content and websites as well.

As per Rule 4(4) of the IL Rules 2021, SSMIs are expected to 'endeavour' to "*deploy technology-based measures, including automated tools or other mechanisms*" to proactively detect information depicting rape, child sexual abuse material (CSAM), or content that is duplicate to information removed earlier by a takedown notice issued under Rule 3(1)(d).

33 https://www.eff.org/wp/caught-net-impact-extremist-speech-regulations-human-rights-content

Additionally, the SSMI would be obligated to display a notice to the users who attempt to access such disabled content. The rule contains three provisos outlining additional safeguards in the deployment of such technology-based measures, which we have discussed in more detail in the subsequent subsections.

**CSAM and material depicting sexual violence**

There seems to be some consensus that certain forms of automated technologies like fingerprinting and hash-matching may be able to successfully detect and remove CSAM.[34] This may be because of the existence of a large amount of corpora with which these tools can be trained.[35] This logic can also be extended to the policing of content depicting sexual violence, since scholars have opined that certain forms of technology-based measures can be utilized to filter out content "that is predetermined to be unlawful."[36]

On the other hand, we must emphasise that any endeavour to filter, monitor and block such content should not be completely delegated to private entities like SSMIs, nor should such operations be continued without due oversight. Content recognition technologies, like the measures envisaged under this provision, have been used historically to detect and report CSAM, including by the NCMEC, an US-based organisation working on these causes. However, as studies show, the endeavour to deploy technology-based measures must be done in consonance with relevant law enforcement authorities, and organisations working to eradicate child exploitation.[37]

Finally, in 2011, the Special Rapporteur to the Human Rights Council, UN General Assembly, had noted that while utilisation of blocking and filtering technology for detection of CSAM may be justifiable, the law making provisions for the same must be precise, and there should be sufficient safeguards, including oversight from an independent and impartial regulatory body.[38]

**Safeguards and oversight**

The aforementioned three *provisos* to the rule further delineate safeguards that the SSMI would be expected to adopt, and includes: a) ensuring that the measures adopted are proportionate to the interests of free speech and privacy of the users, b) implementation of proper human oversight, including a periodic review of such automated tools, and c) ensuring

34 https://www.ofcom.org.uk/__data/assets/pdf_file/0028/157249/cambridge-consultants-ai-content-moderation.pdf

35 New America, Content Moderation - https://www.newamerica.org/oti/reports/everything-moderation-analysis-how-internet-platforms-are-using-artificial-intelligence-moderate-user-generated-content/the-limitations-of-automated-tools-in-content-moderation/

36 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3521619

37 https://www.missingkids.org/content/dam/missingkids/pdfs/ncmec-analysis/grp.pdf

38 https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

that such review looks into the accuracy and fairness of such tools, the propensity of bias and discrimination in these tools, and the impact on their privacy and security. However we do note that the first *proviso* to the rule, regarding ensuring that the tools operate proportionately to user safeguards, is couched in broad terms. As an operational safeguard therefore, it might not amount to a functional test for automated tools. Additionally, we note that these provisos do not make any provision for an aggrieved user to challenge removals via technology-based measures.[39] While the third proviso makes a reference to the need for assessing the accuracy of the tools deployed by the concerned SSMIs, this does not directly translate into a need for the SSMI to actually rectify erroneous removals real-time.

**Content Takedown under the Copyright act**

Copyright is provided to owners of content to gain monetary benefits arising from their world. In case there is an infringement of copyright, there are remedies provided in law against the infringer of copyright and for the benefit of the owner. There is infringing content on websites and other online content. In such a case, TSP's need to block infringing material under the IT Act as well as the Copyright Act. One of the conditions for availing safe harbour is to ensure that content is not infringing copyright and is unlawful. Usually, the copyright owner or licensee requests the injunction remedy. Injunctions are issued by courts against Rogue Websites. When determining whether a website qualifies as a rogue website or not, the courts have taken two distinct stances. The broader approach is used when injunction is passed against an entire website rather than against some specific content while the narrower approach is when an entire website is blocked only if the website solely hosts infringing content. An illustration is when for example, a blog hosts some original and some infringed content, under the broader approach, the entire blog would be blocked while under the narrower approach only the infringing content will be blocked.

## Generative AI advisories

The Ministry of Electronics and Information Technology(MEITY) had issued an advisory on 1st March 2024 right before the announcement of 2024 general elections for observing compliance by intermediaries on AI models, LLM's and Generative AI software. The advisory was later pulled back.

The rolled back advisory stated that - there needs to be explicit permission of the Government for deployment of untested AI models hinting at something akin to the licensing regulation. It also required platforms to deploy a pop up requirement to inform users that the generative answers may be unreliable. It also stated a form of metadata requirement. There was also a mention of an action taken report due within 15 days.

39 https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=26385

The advisory was pulled back on March 15th after heavy criticism.[40]

## Conclusion

As discussed, there continues to be flaws with the regulatory scheme that empowers the government to order content takedown. With respect to the procedure under section 69A, for instance, there are demonstrable harms against public participation that arise out of an opaque, ad-hoc legal blocking and takedown regime.[41] In such light, the *Tanul Thakur* case and Twitter India's lawsuit together may hold the potential for a new era of content takedown regime in India, depending on the ultimate outcome of the cases.

There have been reports of a new Digital India Act coming in to replace the Information Technology Act, 2000 for some time now. A draft is yet to be seen but there have been some public consultations around it. The hope around the new act is that it will bring in more transparency around the content takedown regime, especially by revisiting a provision like Rule 16 of the Blocking Rule.

However, this optimism must be taken with a pinch of salt. Online platforms like Twitter also represent the consolidation of power to censor and shape public discourse on the "*digital public sphere*."[42] There remains a critical lack of examination of the role of internet companies, their design choices[43] and policy decisions[44], responsible for skewing political conversations, harming democratic processes and reinforcing social hierarchies[45]. Such examination is even more critical in non-Western markets, and fledgling and developing democracies.[46]

**40** https://www.thehindu.com/sci-tech/technology/it-ministry-replaces-ai-advisory-drops-requirement-of-governments-permission/article67957744.ece

**41** https://www.icnl.org/wp-content/uploads/4.-Platform-Governance-India-report.pdf

**42** https://www.supremecourt.gov/opinions/16pdf/15-1194_08l1.pdf

**43** https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3132758

**44** https://harvardlawreview.org/wp-content/uploads/2019/12/497-541_Online.pdf

**45** https://www.telegraphindia.com/india/why-supreme-court-lawyer-sanjay-hegde-wants-to-fight-twitter/cid/1717572

**46** In India, for instance, anti-caste scholars and activists have routinely flagged platform inaction in combating vitriolic, casteist hate speech encountered by its users on a daily basis, see: https://cis-india.org/internet-governance/blog/online_caste-hate_speech.pdf

# Surveillance

Surveillance refers to the "*focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction*".[47] In its basic sense, surveillance includes activities which enable the state, or corporations, to manage a population, via the former watching over the latter.[48] Inevitably, this also means that there is an imbalance of power, where the surveillor holds the power to decide the extent to which an individual's data can be collected, controlled and used for 'public good.'[49]

In India, a series of legislations — several of them dating back to the colonial era — enable the government to surveil its citizens, over a variety of purportedly legitimate state functions. These functions include the preservation of security, prevention or investigation of crime, and maintenance of law and order, and often involve the access to and use of an individual's personal data.[50] Legitimate as these functions can be, it must also be noted that the practice of government surveillance is a deeply invasive intrusion into a person's life and conflicts with their fundamental rights, most notably their entitlement to the fundamental right to privacy. The problems that surveillance poses, as a potential violation of individual liberties, is even more pronounced in the current day and age, where technological advancements have made mass-surveillance — involving large-scale collection, processing and analysis of data — more accessible to governments. Therefore, it is critical that the regulatory framework that empowers the government to carry out surveillance ascribes to established legal processes.[51]

This principle was recognized in the 2017 judgement of *Puttaswamy v Union of India*, where the Supreme Court acknowledged that the right to privacy was a fundamental right under the Indian constitution. The judgement of *Puttaswamy* was particularly important for its emphasis on the different conceptions of privacy that vests within the fundamental right to privacy. There are two conceptions that are of interest in the context of surveillance:

a) **Information Privacy**: Informational privacy refers to the expectations of privacy that individuals have with respect to information about them and is linked to the idea of control that individuals should have over their personal information.[52] The court noted that any restraints on informational privacy (as well as other conceptions of privacy), must fulfil a three-fold requirement:

47 Surveillance Studies: An Overview, David Lyon - https://www.researchgate.net/publication/26526923_David_Lyon_Surveillance_Studies_An_Overview

48 https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/pub_dom/pub_dom

49 https://cis-india.org/internet-governance/blog/essay-watching-corona-or-neighbours-introducing-2018lateral-surveillance2019-during-covid201919

50 https://macrofinance.nipfp.org.in/PDF/BBPR2018-Use-of-personal-data.pdf

51 Id

52 https://cis-india.org/internet-governance/blog/the-fundamental-right-to-privacy-an-analysis

i) there must be a law in existence to justify an encroachment on the right (legality),

ii) there must be a legitimate state aim behind the encroachment, so as to ensure that the law falls within the zone of reasonableness mandated by Article 14 (legitimate aim), and

iii) the means through which this encroachment is carried out, is proportional to the object sought to be fulfilled by the law (necessary and proportional).

In addition, through the different opinions in the case, the judgement converged on the principle of informed consent, as the backbone of informational privacy.[53] In particular, the court held that: "*The State must ensure that information is not used without the consent of users and that it is used for the purpose and to the extent it was disclosed.*"[54]

b) **Decisional autonomy**: The court also emphasised on the exercise of individual liberties forming the bedrock of the right to privacy. Three values — dignity, decisional autonomy and integrity (both physical and mental) — formed essential facets of the right, and derived their sources from the broad constitutional framework[55], including the Preamble, Article 21, as well as the entirety of Part III of the Constitution, which guarantees fundamental rights.[56] In particular, Justice Chandrachud found autonomy as empowering individuals to reserve a private space for themselves, to make choices, and assert and make decisions on intimate matters.[57] The right to intimate decision-making further found echoes in the opinions of both Justice Chelameshwar and Justice Nariman.[58] Additionally, Justice Chandrachud located the ability to preserve one's right to preserve their integrity to the value of autonomy, since it was impossible to exercise autonomy without having the control over one's bodily and mental integrity.[59]

In this section, we go over the legislations that empower the government to surveil and/or monitor citizens. While several of these legislations were enacted before the judgement of *Puttaswamy*, the standards laid down there are useful benchmarks for measuring the constitutionality of these legislations nevertheless.

**53** https://indconlawphil.wordpress.com/2017/08/30/the-supreme-courts-right-to-privacy-judgment-iv-privacy-informational-self-determination-and-the-idea-of-consent/

**54** Right to Privacy Judgement Para 70, Justice Kaul

**55** Gautam Bhatia, 'The Supreme Court's Right to Privacy Judgment - I: Foundations' (Indian Constitutional Law and Philosophy, 27 August 2017) https://indconlawphil.wordpress.com/2017/08/27/the-supreme-courts-right-to-privacy-judgment-i-foundations/

**56** https://cis-india.org/internet-governance/blog/the-fundamental-right-to-privacy-an-analysis

**57** Right to Privacy Judgement Para 168 (Chandrachud)

**58** Right to Privacy Judgement Para 81 (Nariman), Para 36 (Chelameshwar)

**59** ibid [168] (Chandrachud J.)

## The Indian Telegraph Act

The Indian Telegraph Act of 1885 ["the Act"] was enacted during the colonial era, and was meant to give the government power to install telegraph lines on private and public property.[60] Since then, however, the law has gone through multiple amendments to accommodate new communication technologies, as evident from the current definition of the term 'telegraph' in the Act. 'Telegraph' is defined as:

> "*any appliance, instrument, material or apparatus used or capable of use for transmission or reception of signs, signals, writing, images and sounds or intelligence of any nature by wire, visual or other electro-magnetic emissions, Radio waves or Hertzian waves, galvanic, electric or magnetic means*."

The interception of such 'telegraph' is further enabled by Section 5(2) of the Act. Section 5(2) sets a two-tiered test that must be satisfied before the Central or State Government can authorise the interception of messages. *Firstly*, there must be a condition of public emergency or an interest of public safety. *Secondly*, the concerned official, who is ordering such interception, must be satisfied that such interception is "*necessary or expedient*" in the interest of the sovereignty and integrity of India, the security of the state, friendly relations with foreign states or public order or for preventing incitement to the commission of an offence. These are grounds listed in Article 19(2) of the Indian Constitution, which prescribes the conditions under which the government can impose reasonable restrictions on the fundamental freedom of speech and expression.

The Telecom Act of 2023 supersedes the Indian Telegraph Act of 1885, the Indian Wireless Telegraphy Act of 1933, and the Telegraph Wires (Unlawful Possession) Act of 1950. Its effective date has not yet been notified. The enactment has stirred controversies concerning both the manner of its passage and the provisions it contains. Unlike Rule 419A which aimed to build safeguards in the interception regime, currently there are no rules which can build in safeguards.

### *PUCL v Union of India*

In 1990, there were a series of political scandals and revelations regarding the ruling government's widespread use of illegal phone-tapping of its opponents. The Central Bureau of Investigation (CBI) released a follow-up report that provided more details around these allegations, including the extent of illegal phone-tapping used during the political turbulence of 1980s and early 1990s, exposing that not only had the previous central government surveilled its opposition, but also its own ministers, and political leaders of many states.[61] The report exposed the inadequacy of India's legal framework and the procedural lapses that

60 https://cis-india.org/telecom/resources/indian-telegraph-act

61 http://nujslawreview.org/wp-content/uploads/2016/12/Chaitanya-Ramachandran.pdf

enabled this practice. Phone-tapping was carried out without proper authorisation, persisted for longer periods than it was permissible under the law, and was not based on legally tenable grounds.[62]

Following these revelations, the People's Union of Civil Liberties (PUCL) filed a writ petition in the Supreme Court, challenging the constitutional validity of Section 5(2) of the Telegraph Act, the provision supposedly in use to order such phone-tapping in the first place. In the alternative that the court found the provision constitutional, PUCL prayed that the court read down the provision to include procedural safeguards to rule out arbitrariness and prevent indiscriminate phone-tapping.

The court chose to adopt the latter approach, refraining itself from declaring section 5(2) as unconstitutional. Instead, it emphasised on the necessity to adhere to the two-tiered test detailed in the Telegraph Act ("occurrence of any public emergency" or "the interest of public safety"), as well as to issue interception orders only on the permitted grounds mentioned in the provision.

It is worthwhile to consider the jurisprudence behind the terms "public emergency" and "public safety", since the court went into detail about the meaning of these terms. The court identified that while the term "public emergency" has not been defined in the Act, the fact that it occurs in consonance with the term "public safety" means that these two terms "*take colour from each other*".[63] The court defined a "public emergency" to mean the prevailing of a sudden condition or state of affairs, that affects the people at large, and that requires immediate action; while "public safety" meant the state or condition of freedom from danger or risk for the people at large.[64]

Constitutional scholar Gautam Bhatia has further argued that these two terms cannot be given widely different meanings, simply because if the threshold for one of the terms was more lax than the other, then the latter would become redundant. This means that if the threshold for considering a situation to be in the interest of "public safety" was more broad than a situation of "public emergency", then the term "public emergency" loses its meaning.[65] Therefore, these two terms must be non-overlapping, referring to different aspects and require roughly the same standard, to be a reasonable ground for the issuance of an interception order.[66]

Finally, the court laid down safeguards to prevent arbitrariness in phone-tapping orders, which included:

62 Id

63 People's Union for Civil Liberties vs. Union of India & Ors. Para 27 (https://indiankanoon.org/doc/31276692/)

64 People's Union for Civil Liberties vs. Union of India & Ors. Para 28 (https://indiankanoon.org/doc/31276692/)

65 https://indconlawphil.wordpress.com/2013/12/18/surveillance-and-privacy-in-india-iv-analysing-the-landmark-pucl-judgment/

66 Id

1) An order for telephone-tapping will not be issued except by the Home Secretary, Government of India (Central Government) and Home Secretaries of the State Governments. In an urgent case the power may be delegated to an officer of the Home Department of the Government of India and the State Governments not below the rank of Joint Secretary. A copy of the order must be sent to the Review Committee, within one week of the passing of the order.

2) The order must require the authorities to intercept only such communications as are described in the order. The order may also require the authorities to whom it is addressed, to disclose the intercepted material to such persons and in such manner as are described in the order.

3) While issuing an order, the authorities must consider whether such an order is necessary under Section 5(2) and whether the information sought can be acquired reasonably by other means.

4) An interception order issued under Section 5(2), will require interception of only communications as specified in the order.

5) The interception order will cease to have effect at the end of a period of two months, unless renewed. The authority which issued the order may, at. any time before the end of the two month period renew the order if it considers that it is necessary to continue the order in terms of Section 5(2) of the Act. The total period for the operation of the order will not exceed six months.

6) Each copy made of any of the intercepted material shall be destroyed as soon as its retention is no longer necessary in terms of Section 5(2) of the Act.

7) There shall be a Review Committee consisting of Cabinet Secretary, the Law Secretary and the Secretary, Telecommunication at the level of the Central Government. The Review Committee at the State level shall consist of Chief Secretary, Law Secretary and another member, other than the Home Secretary, appointed by the State Government:

a) The Committee shall on its own, within two months of the passing of the order by the authority concerned, investigate whether there is or has been a relevant order under Section 5(2) of the Act, and whether there has been any contravention of the provision.

b) If on an investigation the Committee concludes that there has been a contravention, it shall set aside the order and direct the destruction of the copies of the intercepted material.

c) If on investigation, the Committee comes to the conclusion that there has been no contravention of the provision, it shall record its finding to that effect.

## The Telegraph Rules

The Indian Telegraph Rules, 1951, further the procedural norms for the substantive framework that had been erected by Section 5(2) of the Act. In 2007, these Rules were amended, and Rule 419A was introduced, which attempted to codify the procedural safeguards laid down by the Supreme Court in the *PUCL* judgement. Notable changes introduced by Rule 419A are as follows:

1) An interception order under Section 5(2) may normally be issued only by the Union Home Secretary at the Centre, or a State Home Secretary at the States. There are two exceptions to this rule:

a) Under "unavoidable circumstances", an order may be issued by an officer not below the rank of a Joint Secretary to the Government of India, who has been authorised by the Union/State Home Secretary to this effect. It must be noted that the phrase "unavoidable circumstances" is not defined anywhere in the statute, and therefore, the contours of this exception are ambiguous.

b) In "emergent cases", where procuring a lawful order is itself infeasible — due to remoteness of location, or for operational reasons — interception may be carried out with the prior approval of the Head or the second senior most officer of the authorised Law Enforcement Agency at the Centre, or officers authorised in this behalf, not below the rank of Inspector General of Police at the States. Orders issued under these circumstances must be communicated to the competent authority within three working days, and confirmed within seven working days.

2) The total period of interception (including renewals of the interception order) is limited to a total of 180 days.

3) The copy of an interception order must be forwarded within 7 working days to the respective Central/State Review Committee, which has been constituted by the Central/State Government under Rule 419A for the purpose of reviewing such orders. The Review Committees will meet at least once in two months and determine if the lawful orders placed before them are in accordance with Section 5(2) of the Telegraph Act. When a Committee is of the opinion that a lawful order is violative of Section 5(2), it may set aside the order and ask that all copies of information intercepted under that order be destroyed.

4) Telecommunications service providers are required to designate two senior executives as nodal officers to receive and handle interception orders. They must acknowledge receipt of the interception order within two hours, and submit a list of all interception orders received to the nodal officers of the requisitioning security and law enforcement agencies for verification.

## The Information Technology Act and Rules

While the ambit of the Telegraph Act presumably extends to interception of calls and messages, the current Indian legal framework also empowers the government to order for the interception of electronic communications via section 69 of the IT Act, and the allied rules. Although the language of section 69 of the IT Act is modelled after the Telegraph Act, there are three distinctions[67]: *Firstly*, the two thresholds listed in the Telegraph Act — that is, an interception order being preceded by a situation of public emergency or public safety — are missing. *Secondly*, the IT Act adds two additional grounds — "defence of India" and "investigation of any offence" — on top of the five grounds listed in the Telegraph Act, under which an interception order can be issued. *Thirdly*, section 69(3) imposes an additional obligation on intermediaries, subscribers and persons in-charge of the computer resource to "extend all facilities and technical assistance" to the intercepting agency.

The procedural framework that governs this interception process under section 69, is legislated by the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 ["the Interception Rules"]. These rules detail the designation of the authority competent to issue an interception order, requiring reasons for such order, providing for duration and review of such orders, and prohibiting disclosure of such information to unauthorised parties.

Finally, section 69B of the IT Act empowers the Central Government to authorise "*any agency of the Government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource*". The threshold for such authorisation is considerably lower than those stated in the Telegraph Act or section 69 of the IT Act, and involve only the "*enhanc[ing] cyber security and for identification, analysis and prevention of any intrusion or spread of computer contaminant in the country*". Traffic data has been given a wide definition under Section 69B(4)(ii) and includes metadata. The Government has also provided a procedural framework for the issuance of directions relating to traffic data under the Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules, 2009. Additionally, rules framed under other provisions of the IT Act also facilitate state surveillance for the purpose of identity verification or for prevention, detection, investigation, prosecution, and punishment of offences.[68]

As has been indicated throughout this section, the provisions of the IT Act empower the government to order for surveillance for grounds that are much wider than those envisaged in the Telegraph Act.[69]

**67** https://macrofinance.nipfp.org.in/PDF/BBPR2018-Use-of-personal-data.pdf

**68** See: SPDI Rules, IL Rules 2021

**69** https://macrofinance.nipfp.org.in/PDF/BBPR2018-Use-of-personal-data.pdf

## Traceability under the IL Rules 2021[70]

The Il Rules 2021, issued under section 79 and section 69A of the IT Act, introduce additional obligations for Significant Social Media Intermediaries (SSMIs) to "*enable the identification of the first originator of the information*", as may be required by a court order or by a order passed under section 69 of the IT Act. This obligation is commonly referred to as a "traceability" requirement, and has gone through many contested debates over the past few years, before becoming the law.

Allowing for the tracing of online communications is a violation of the fundamental right to privacy. Applying the framework by Bhandari et. al[71], that condenses the Supreme Court's judgments on the right to privacy, we examine the suitability and necessity of this rule with respect to the purpose it aims to serve, and balancing of the right and the need to interfere thereinto.

**Legality:** The introduction of the traceability requirement through the IL Rules 2021 is an exercise in delegated legislation, which allows the government to make binding laws with the necessity to pass a legislation through the Parliament. However, nothing in sections 69A and 79 of the IT Act, which empower the traceability requirement, envisions a state power to infringe upon privacy in the rules. Even the IT Act as a whole does not empower the Government to mandate technical changes to platforms. Therefore, as the parent provisions do not explicitly authorise any privacy-infringing power, the introduction of the traceability requirement through delegated legislation does not adequately fulfil the test of legality.[72]

**Legitimate aim**: The rule states that an order to trace the first originator can be passed for the "prevention, detection, investigation, prosecution or punishment of an offence related to the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, or public order"; or of "incitement to an offence relating to the above or in relation with rape, sexually explicit material or child sexual abuse material, punishable with imprisonment for a term of not less than five years."[73] While these grounds are expansive, they are still legitimate grounds for surveillance.[74]

70 This section is taken from CIS' earlier commentary on the IL Rules 2021. The full commentary can be found here: https://cis-india.org/internet-governance/legality-constitutionality-il-rules-digital-media-2021.
Additionally CIS researchers have authored a legal analysis of the traceability requirement separately, which also informs this analysis, and can be accessed here: http://nujslawreview.org/wp-content/uploads/2021/07/14-2R-The-Ministry-and-the-Trace-Subverting-End-to-End-Encryption.pdf

71 http://ohrh.law.ox.ac.uk/wordpress/wp-content/uploads/2020/05/U-of-OxHRH-J-The-Surveillance-State-Privacy-and-Criminal-Investigation-1.pdf

72 http://nujslawreview.org/wp-content/uploads/2021/07/14-2R-The-Ministry-and-the-Trace-Subverting-End-to-End-Encryption.pdf

73 Intermediary Rules, 2021 Rule 4(2)

74 Vrinda Bhandari and Karan Lahiri - https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3580630

**Necessity and Proportionality**: This test assesses whether the privacy-infringing measures are capable of achieving the ends pursued, and whether there are alternatives with lesser degree of limitation that can achieve the same ends.[75]

For the first part of the test, we must understand what are the ostensible aims with which the traceability requirement was set up. The press note that had accompanied the notification of the rule outlined the government's rationale: proceedings in the Supreme Court that asked the Government to frame guidelines to eliminate online child sexual abuse and rape related content (see: In *re Prajwala* for a discussion of the case); a Calling Attention Motion in the Rajya Sabha on disinformation leading to violent lynchings, to which the Ministry had promised amending the rules to include traceability; and the Report of the Ad-hoc Committee of the Rajya Sabha that recommended breaking end-to-end encryption so that originators of child sexual abuse material could be traced.[76]

Assuming that these are the aims with which the government intends to enforce the requirement, traceability would not be able to achieve the ends pursued. As pointed out by researchers, all traceability implementations suffer from critical limitations that prevent it from achieving this goal, and also pose operational difficulties for messaging services.[77] In addition, traceability mandates can also be easily circumvented by motivated individuals, which cast further aspersions on the suitability of adopting traceability requirements for achieving the described aims.

For the second part of the test, we must assess if traceability is necessary for the purposes described by the government. It must be noted at the outset that the government has not presented any evidence that the amount of data (and the current surveillance powers) are inadequate to counter the issues that traceability is meant to solve.[78] In addition, there also exists other methods by which service providers can identify bad actors, including the collection of metadata and proactive monitoring of unencrypted user data. These methods can be considered a more proportionate means to the end, as opposed to traceability, which compels compromising with every user's privacy and security.[79] As such, it is difficult to understand how traceability can fulfil the test of necessity, where it is the least restrictive way to aid the government on its purported aims.

**75** *Puttaswamy*

**76** Ministry of Electronics and Information Technology, Government notifies Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, Press Information Bureau, February 25, 2021, available at https://pib.gov.in/PressReleseDetailm.aspx?PRID=1700749

**77** http://nujslawreview.org/wp-content/uploads/2021/07/14-2R-The-Ministry-and-the-Trace-Subverting-End-to-End-Encryption.pdf

**78** Id

**79** Id

## Code of Criminal Procedure, 1973

Section 91 of the Code of Criminal Procedure (CrPC) empowers a Court or any officer in charge of a police station to summon any document or any other thing from a person, if it is necessary or desirable for the purposes of any investigation, inquiry, trial or other proceeding under the Code. This provision has been used by the police to seek information from intermediaries, or access stored data.[80]

Section 92 regulates the interception of a document, parcel or thing in the custody of a postal or telegraph authority.[81]

## New Criminal Laws

Akin to Section 91 of CrPC under Chapter VII is the law related to production of documents. Section 94 of BNSS, enables authorities to summon documents, electronic communication etc for the purpose of investigation. There isn't much change here from the CrPC.

## The Criminal Procedure (Identification) Act, 2022

The Criminal Procedure (Identification) Act, 202 ["the CPI Act"]2, was enacted in April, 2022, and seeks to authorise the collection, analysis and storage of "measurements of convicts and other persons" for "identification and investigation in criminal matters and to preserve records".[82]

### What does the Act say?

Section 2(b) of the CPI Act define "measurements" as including "finger-impressions, palm-print impressions, foot-print impressions, photographs, iris and retina scan, physical, biological samples and their analysis, behavioural attributes including signatures, handwriting or any other examination referred to in section 53 or section 53A of the Code of Criminal Procedure, 1973".

The examinations under Section 53 of the CrPC include that of "blood, blood stains, semen, swabs in case of sexual offences, sputum and sweat, hair samples and fingernail clippings by the use of modern and scientific techniques including DNA profiling...". Additionally, section 53A provides for the recording of additional particulars, including, age of the arrestee and marks of injury on their person.

**80** https://macrofinance.nipfp.org.in/PDF/BBPR2018-Use-of-personal-data.pdf

**81** https://www.icnl.org/wp-content/uploads/5.-Surveillance-India-report.pdf

**82** Statement of Objects and Reasons, The Criminal Procedure (Identification) Act, 2022

Section 3 of the Act allows the police or a prison officer to compel certain classes of people to give their "measurements", which includes persons convicted under any offence, persons detained under preventive detention laws and all persons arrested for an offence. For the latter category, such persons can be compelled to provide all measurements, except biological samples. The provision carves a further exemption to this, stating that persons who have been arrested for offences against women or children, or for offences that are punishable with imprisonment of seven years or more, can be compelled to provide biological samples as well.

At this juncture, it must be noted that the Act contemplates two distinct concepts[83]: One, 'measurements', as defined above, include the biological samples and other personal information. Two, the Act also mentions the concept of 'records of measurements', which includes the records and documentation of the measurements compiled subsequent to the taking of the measurement itself.

This distinction is important to understand, because the CPI Act has different stipulations for collection, storage and dissemination of "measurements" and "records of measurements". Section 4(1) states that the National Crime Records Bureau (NCRB) can, in the interest of prevention, detection, investigation and prosecution of any offence: a) collect records of measurement from the governments of states or union territories, b) store, preserve and destroy the record of measurements at national level (c) process such record with relevant crime and criminal records and (d) share and disseminate such records with any law enforcement agency. Section 4(2) states that such records of measurement can be stored digitally or electronically for seventy-five years. Finally, section 4(3) states that the State Government and Union Territories may notify the appropriate agencies who may collect, preserve and share the measurements in their respective jurisdictions.

In addition to empowering police and prison officers from collecting measurements, section 5 empowers a Magistrate to also authorise "any person" to give their measurements, if the Magistrate is satisfied that it is expedient to do so for the purpose of any investigation or proceeding under the CrPC or any other law.

The CPI Act makes provisions should a person refuse to give their measurements. Section 6(1) of the Act states that a police or a prison officer can compel the giving of measurements, as might be prescribed, while section 6(2) makes it a punishable offence to refuse the giving of such measurements.

## Critical analysis of the Act

The enactment of the CPI Act has been met with widespread criticism. One of the provisions that has squarely drawn criticism has been section 6, which criminalises the refusal to provide measurements. This violates the right to life, as guaranteed by Article 21, in a variety of ways.

83 https://static1.squarespace.com/static/5a843a9a9f07f5ccd61685f3/t/634d22c3b82adb425792 6c79/1665999595973/P39A+Brief+-+Criminal+Procedure+%28Identification%29+Act%2C+2022+%281%29.pdf

*Firstly*, as has been held in *Puttaswamy*, decisional autonomy and bodily integrity, that is, the right to make choices, is protected as a constitutional guarantee under Article 21. Compelling an individual to produce their measurements, against their will, is a violation of an individual's right to choice, and goes directly against the direction of the court in *Puttaswamy*.

*Secondly*, this violation becomes even more egregious when one considers section 5 of the CPI Act allows the Magistrate to compel "any person" to give their measurements, and not merely persons convicted, detained or arrested for an offence. In the Statement of Objects and Reasons of the Act, it is mentioned that the collection of these measurements will make criminal investigations more efficient, by increasing the conviction rate. However, as has been argued elsewhere, this increase of conviction will come at the cost of those individuals who are already marginalised, because of their socio-economic positions in a stratified society like India's.[84] As delineated in *Puttaswamy*, a restriction against the right to privacy must fulfil the test of legality, legitimate aim and necessity and proportionality. It is difficult to reconcile how such a wide net cast by section 5, where any person can be compelled, at the threat of an offence, to produce their measurements, can meet the requirement of legitimate aim or that of necessity and proportionality.

*Thirdly*, consent does not feature as an element in any of the provisions. As *Puttaswamy* displayed, the State was constitutionally bound to take an individual's "*informed, meaningful consent at every stage that it wants to use that individual's information*."[85] This means that the State is obligated to obtain consent for each instance in which it intends to use an individual's data. However, not only does the CPI Act does not stipulate that an individual's consent is required before collecting their measurements, it actively works to erode individual consent, by criminalising their refusal.

Currently, the constitutional validity of multiple provisions of the CPI Act is being challenged at the Delhi High Court. The petitioners in the case have stated that the provisions are arbitrary, excessive, unreasonable, disproportionate and in violation of fundamental rights of the citizens of India.[86]

## Conclusion

Much like the state of surveillance in India pre-*PUCL*, the Indian government has allegedly continued to exercise surveillance and interception practices that do not have any basis in any of the laws delineated above. For instance, in 2018, Citizen Lab, a Canada-based laboratory,

**84** https://theprint.in/opinion/criminal-procedure-acts-grand-tech-vision-comes-with-dangers-of-police-power-data-violation/925952/

**85** https://indconlawphil.wordpress.com/2017/08/30/the-supreme-courts-right-to-privacy-judgment-iv-privacy-informational-self-determination-and-the-idea-of-consent/

**86** https://thewire.in/law/explainer-why-the-criminal-procedure-identification-act-is-being-challenged-in-court

released a report detailing the capabilities of a spyware called Pegasus, produced by an Israeli Firm named the NSO Group. Their report detailed that the spyware could compromise the digital divide of an individual without requiring any action on the part of the target of the software. Once the software had infiltrated the device, it had the capacity to access the entire stored data on the device, it had real-time access to emails, texts, phone calls and multimedia recording capabilities of the device. The report also detailed that the NSO group purportedly only sold this software only to undisclosed governments, and that the users of this software were "*exclusively government intelligence and law enforcement agencies*", as was apparent on their own website.[87]

As a continuation of this through 2020 and 2021, the Citizen Lab, as well as Amnesty International and a consortium of journalistic organisations around the world, released results of various investigative endeavours, that showed that among the people allegedly targeted by Pegasus, a considerable number of them were Indians. These Indians included senior journalists, doctors, political persons and even some Court staff.

These discoveries led to a batch of petitions being filed in the Supreme Court of India, where the Indian government was impleaded as the respondent. The petitions raised the issue of inaction on the part of the government to consider the allegations raised, and also expressed the apprehension that given that the NSO Group's own disclosure stated that they only sold their product to governments, either foreign government or certain Indian governmental agencies were using this software to surveil on their own citizens without due procedure under the law.

In 2021, the court observed that, despite repeated requests to the government to address the claims made in the petitions, the government only continued to provide limited information, which did not shed any light on their stand or provide any clarity as to the facts. In such light, the court found that the materials placed by the petitioners on record made out a *prima facie* case that merited the court's consideration. The court directed the formation of an Expert Committee, that would be headed by a Supreme Court judge and experts in cyber security, who were tasked to provide their recommendations in front of the court subsequently.

In October, 2023, many noteworthy figures such as journalists, leaders of the opposition party received notifications from Apple that 'State Sponsored Attackers were targeting their I-phones'. In a public statement, Apple said that the warnings could be a false attack as well.[88]

India recently passed the Personal Data Protection Act in the Monsoon session of parliament. The Act  makes no mention of surveillance. The previous versions of the bill did mention the term and defined Surveillance as a harm as well.  It is crucial to acknowledge the negative effects of surveillance and guarantee that governmental monitoring will be kept to a minimum through suitable procedural safeguards in order to preserve citizens' confidence in the

**87** https://main.sci.gov.in/pdf/LU/27102021_082008.pdf

**88** https://www.nytimes.com/2023/11/01/world/asia/india-apple-threat-notification.html

protection of their personal information. The law does not provide any remedies against over broad surveillance and also dilutes the Right to Information Act.

As we await further developments in this case, this might be a good time to reform our existing surveillance legal framework. Given the fact that several of the existing surveillance legislations — the Telegraph Act, the CrPC, and select provisions of the IT Act — were enacted before the pronouncement in *Puttaswamy*, there does not currently exist any jurisprudence that seeks to rethink the constitutionality of these legislations. Nevertheless, in light of the judgement, it is imperative for courts and policymakers to rethink whether these legislations are compatible with the threefold test delineated in *Puttaswamy*, and accordingly update these laws to reflect the modern standards of privacy. For instance, policymakers and courts must consider whether the fact that the Telegraph Act does not have the requirement for judicial oversight over interception orders, can be grounds for section 5(2) to be incompatible with *Puttaswamy*. Some limited evidence would answer this question in affirmative. For instance, post-*Puttaswamy*, a surveillance provision in the Aadhaar Act was struck down by the Supreme Court in Aadhaar because it only required executive application of mind (and did not have judicial oversight).[89] Therefore, a rethinking of the surveillance legislations that were enacted pre-*Puttaswamy*, is necessary.

**89** Bhandari and Lahiri

# Device Seizures

The right to conduct a search and seizure of persons or places is an essential part of investigation and the criminal justice system. In India, the criminal procedure code grants an almost unfettered power to investigative agencies to search, sometimes even in the absence of a warrant. Section 165, for instance, allows a warrantless search in case it is immediately needed to prevent loss or fabrication of relevant evidence in a case.[90] Although this section is meant to work as an exception to the norm, recent cases indicate that this wide power is often used arbitrarily to circumvent due process of the law.[91] Another challenge is that illegally obtained evidence is usually still admitted in court in India, as long as it is relevant.[92] Since there aren't specific provisions that bar the admissibility of such evidence, Indian courts have held that the discarding of due process is no more than an irregularity.[93]

With the growing importance of digital devices in citizens' lives, law enforcement has also begun to rely heavily on digital evidence. Smartphones, for instance, can contain a complete record of the communications data, photos, videos and documents, of a user, along with other personal information, like application data, location tracking, or financial data. However rules regarding search, seizure and admissibility of electronic evidence do not address this vulnerable nature of digital evidence.

## Background

The Code of Criminal Procedure and the Information technology Act together empower investigation agencies to seize digital and electronic devices. In light of the recent crackdown on the independent news outlet, Newsclick.in[94], it can be deduced that device seizures can take place under UAPA as well. Where there is not a clear jurisprudence on the exact laws and legislations under which device seizures can take place, currently we see them taking place under the Income Tax Act, UAPA, Prevention of Money Laundering Act and during regular investigation.

The Criminal Acts in India namely The Criminal Procedure Code, The Evidence Act as well as the Indian Penal Code have been overhauled and replaced by **Bharatiya Nagarik Suraksha Sanhita, 2023, Bharatiya Nyay Sanhita, 2023, and Bharatiya Sakshya Adhiniyam, 2023** which will be effective **July 1, 2024**. It is yet to be seen how these laws will impact device seizures.

**90** Section 165, Criminal Procedure Code, 1973.

**91** https://article-14.com/post/laws-around-electronic-evidence-compromise-india-s-criminal-justice-system

**92** Vrinda Bhandari, Karan Lahiri, "The Surveillance State, Privacy and Criminal Investigations in India: Possible Futures in a Post-Puttaswamy World," University of Oxford Human Rights Hub Journal 3(2).

**93** Amar Singh vs Balwinder Singh & Ors, Appeal (crl.) 1671 of 1995; Dhanaj Singh alias Shera And Ors v. State Of Punjab 2004(2) SCR 938; Sri Sambhu Das alias Bijoy Das & Anr vs State Of Assam AIR 2010 SC 3300.

**94** https://thewire.in/media/weeks-after-unprecedented-raids-newsclick-staffers-grapple-with-waiting-game

## Code of Criminal Procedure

The Criminal Procedure Code sets out how searches and seizures for criminal investigations can be conducted. The police have powers to search/seize residents' property, including mobile phone and computer devices, both with or without a warrant (although in the latter case, they are required to record reasons in writing for such search).

The following sections have been used by police to apply to the seizure and unlocking of electronic devices:

**Section 91, Cr.P.C:** Allows the police and magistrates the power to compel any person to produce "any document or other thing" that is "necessary or desirable" for the purposes of "any investigation, inquiry, trial or other proceeding under this Code." This can extend to a person's mobile phone, if the police think it is "necessary or desirable" for the investigation of an offence.

**Section 93, Cr.P.C:** Governs the issue of search warrants. Here, the court can issue a search-warrant if (a) it considers that a person will not produce a document / thing as directed under Section 91, Cr.P.C., or; (b) where that document / thing is not known to be in the possession of any person, or; (c) where "the purposes of any inquiry, trial or other proceeding under this Code will be served by a general search or inspection".

**Section 94:** Confers powers on a magistrate to issue a warrant to authorise the police to search any place suspected to contain stolen property, forged documents, etc.

In a case before the High Court of Karnataka in 2021, the court clarified that that word "place" in Sections 93 and 94 extend to a digital device (in that case, a mobile phone).

**Section 100:** In the event the place to be searched is closed, the person residing in or in charge of the place is required to allow the officer executing the warrant to enter and search, on production of such warrant.

**Section 100 of the Code of Criminal Procedure** also lists down the manner in which the person will be searched.

1) When a search warrant is produced, the person residing in the place to be searched should reasonably assist the investigating officer in the search.

2) In case it is suspected that documents or objects are being concealed, the investigating officer can do a physical search of the person. In case of a woman, the search has to be conducted by a woman officer.

3) Two or more independent and respectable residents of the locality should be present during such a search. The search will be done in their presence and a list of things as well as the place that were found in would be made in their presence and they will be required to sign it.

4) A list of things searched and seized will be given to the resident or a person appointed by him. The resident and the person have the right to be present during a search.

5) In case the resident refuses or neglects to attend the search, he//she shall be deemed to commit an offence.

**Section 102:** Confers powers upon police officers to seize property "alleged or suspected to have been stolen" or "found under circumstances which create suspicion of the commission of any offence", and details the procedure consequent to any such seizures, including mandated reporting to the relevant magistrate. Importantly, this does not require a prior warrant.

**Section 165:** This section allows the police greater power to conduct searches in the absence of search warrants, when there is a perceived urgency in the matter. It confers power upon a police officer, to conduct a warrantless search of a place if he has reasonable grounds for believing that "anything necessary for the purpose of an investigation into any offence" may be found in such a place, which "cannot be otherwise obtained without undue delay". In the exercise of this power, the police officer is required to record in writing the grounds for such belief, and as far as possible, identify the item for which search is to be made.

**Section 132 of the Income Tax Act** gives the power of search and seizure to Income Tax officers. In case an accused or a person who is summoned does not produce the required documentation even after the issue of a notice for any proceedings under the Income Tax Act.

1) The authorised person can search any premises.
2) Break open any doors, locks, boxes etc.
3) Seize any books of accounts, documents, articles etc.
4) Make a note/inventory of seized material.

## New Criminal Laws

In the new law, **Section 94 of the Bharatiya Nagarik Suraksha Sanhita, 2023**, empowers both the court and the designated police officer to request any document or item deemed necessary for an investigation to be presented as evidence. Notably, this proposed legislation explicitly encompasses the summoning of digital evidence, encompassing electronic communications like messages, call recordings, and emails, as well as electronic devices such as mobile phones, laptops, cameras, and any other electronic devices that may be specified by the government through future notifications. Additionally, the court reserves the authority to issue orders for the search and seizure of such evidence for various reasons, particularly if

the individual in possession of the evidence is unlikely to voluntarily produce it.[95] A caveat in such proceedings is that the entirety of data pertaining to an investigation may be available in a device.

There is an expansion of the term document under Bharatiya Sakshya (Second) Act, 2023 to bring in any electronic devices including laptops, mobile phones etc. There is also a lack of proper safeguards in place to govern these devices. Section 94 of the Bharatiya Nagarik Suraksha Sanhita (BNSS), akin to Section 91(1)(3) of the Code of Criminal Procedure (CrPC), grants the authority to a Court or a police station's designated officer to summon electronic communications suspected to harbour digital evidence.

Section 94 of the BNSS has come up with provisions regarding the introduction of electronic communication, encompassing communication devices that might contain digital evidence. The section breaks the procedures for acquiring documents, electronic communications, and other items deemed necessary for investigation, trial, or proceedings under the BNSS. In such cases A designated court or an investigating officer can issue a summons to an accused in possession of incriminating material, directing them to produce the specified materials at a designated time and place. Such summons can be issued in physical or electronic form respectively. In cases an accused may only present the document rather than appearing in person. There is a risk of manipulation of data in such cases. There needs to be sufficient safeguards in place to ensure that individuals privacy does not get compromised in such proceedings.[96]

A safeguard that comes in place here mandated by the BNSS is the mandatory videography of the search and seizure procedures which also include putting together the list of seized items as well as signature by witness. There are per say not guidelines given for such recordings but they can be conducted using a mobile device and subsequently forwarded to court of law. This is highlighted in Section 185 of the act. It additionally also requires the maintenance of a case diary and the records created under search need to be sent to a competent authority within 48 hours of the search.[97]

## Precedent, case law, and current position

Since device seizures are typically done in the course of criminal investigations, questions of its legality arise from protections granted to persons suspected of, or accused of, crimes.

**95** https://www.medianama.com/2023/11/223-device-seizure-right-to-privacy-derek-obrien-dissent-note/

**96** https://prsindia.org/billtrack/the-bharatiya-nagarik-suraksha-sanhita-2023

**97** https://www.livelaw.in/top-stories/use-of-audio-video-electronic-means-for-investigation-trial-according-to-bnss-246726

### Article 20(3)

Constitutional questions of the government's right to seize devices and use it in criminal investigations stem largely from Article 20(3) of the Constitution of India, which guarantees a fundamental right against self incrimination.

"No person accused of any offence shall be compelled to be a witness against himself"

This is typically read with Article 21, which grants a broader fundamental right to life and liberty that can only be limited by procedure laid down by the law. In 1978, through *Maneka Gandhi v. Union of India*[98], the Supreme Court added an important qualifier to this right, interpreting that the procedure envisaged by Article 21 must be just, fair and equitable.

## *M.P Sharma v. Satish Chandra*

Compelling suspects to allow access to their device is a more recent development that stems from previous investigative practices that violate privacy such as searching homes, taking fingerprints or voice samples, etc. Their protection lies in three important phrases in Article 20(3), "accused of any offence", "compelled" and a "witness against himself," that have been interpreted differently by the Supreme Court over the years.

In M.P. Sharma vs Satish Chandra, the Supreme Court was tasked with determining if a search and seizure under Sections 94 and 96 of the 1898 Criminal Procedure Code violated Article 20(3) of the Constitution. Article 20(3) was initially envisioned to protect people accused of a crime, or otherwise in police custody, from being compelled to confess, and therefore it was unclear if this extended to search and seizure operations.

At the outset, Jagannadhadas J. clarified that

> "*The fundamental guarantee in article 20(3) comprehends within its scope not merely oral testimony given by an accused in a criminal case pending against him, but also evidence of whatever character compelled out of a person who is or is likely to become incriminated thereby as an accused. It, therefore, extends not only to compelled production of documents by an accused from his possession, but also to such compelled production of oral or documentary evidence from any- other person who may become incriminated thereby as an accused in future proceedings*."

Through this, the court agreed with the petitioner's arguments that a forcible search and seizure was simply an indirect way of accomplishing what Article 20(3) forbade – obtaining self-incriminating testimony from an accused. The court held that the meaning of the phrase "to be a witness", under Article 20(3), was analogous to "to furnish evidence". As a result, the fundamental protection under Article 20(3) would extend to cases where the accused was asked to furnish evidence.

**98** Maneka Gandhi v. Union of India, AIR 1978 SC 597.

## *State of Bombay v. Kathi Kalu Oghad*

In 1961, this position came to be challenged before an 11-judge bench of the Supreme Court in Kathi Kalu Oghad. The question before the court was whether fingerprints and handwriting samples were testimony or evidence that was protected by Article 20(3).

More specifically, the court had to answer whether compelling an accused to provide their fingerprints, or a handwriting sample, was equivalent to compelling them to be a "witness" against themselves. This judgement provides the most definitive interpretation of the phrase "*to be a witness against himself*".

Stressing on the implications this could have on the efficiency of criminal investigations, the majority held the protection guaranteed under Article 21 could not have been intended to obstruct investigations.

> "*... though they may have intended to protect an accused person from the hazards of self- incrimination, in the light of the English Law on the subject – they could not have intended to put obstacles in the way of efficient and effective investigation into crime and of bringing criminals to justice. The taking of impressions or parts of the body of an accused person very often becomes necessary to help the investigation of a crime.*"

As a result, they created a distinction that separates fingerprint and other evidence from witness "testimony."

> *"To be a witness" means imparting knowledge in respect of relevant facts, by means of oral statements or statements in writing, by a person who has personal knowledge of the facts to be communicated to a court or to a person holding an enquiry or investigation."*

Thus, the majority held that to be a witness meant to communicate **personal knowledge** of a relevant fact. Taking immutable physical evidence in the form of fingerprints or handwriting samples, which cannot be altered by the individual, does not make them a witness against themselves, and therefore such information would not be violative of Article 20(3)'s protection.

Another distinction was provided by this case, between physical evidence that did not get the protection of 20(3) and witness testimony: "Physical evidence" is only relevant for purposes of comparison and so by itself it is not incriminating; since police only take the sample to compare it with other material. "Testimonial compulsion" is incriminating by itself, and conveys to the police information that is the direct product of testimony. Thus, even if an individual was compelled to provide their fingerprints, or blood samples, they were being made to be a witness '*against themselves*'. This is because the fingerprint, or the blood sample was not in itself incriminating the individual. Rather, it becomes incriminating only when such information is successfully matched with another piece of evidence. Therefore, providing such information in itself, was not self-incriminatory.

In summary: This judgement concluded that Article 20 (3) only protected the accused against being forced to convey information based on her 'personal knowledge', and did not protect against giving 'material evidence', as such material evidence only lent itself to comparison, as opposed to having the tendency to directly incriminate the accused.

## *Selvi v. State of Karnataka*

In 2010, in *Selvi v State of Karnataka*, the Supreme Court was called to re-examine the scope of Article 20(3). This case came to the Supreme Court on appeal when in the course of an investigation, accused persons, suspects and witnesses were subjected to neuro-scientific tests without their consent. The constitutionality of three investigative techniques: narco-analysis, the polygraph test, and the Brain Electrical Activation Profile, was the primary question before the court.

In narco-analysis, an intravenous injection of a drug into a subject's blood-stream sends them into a hypnotic state, lowering their inhibitions, and making them more likely to divulge information. A polygraph test, on the other hand, measures various physiological responses (respiration, blood pressure, blood flow etc.) during questioning, and makes determinations about the truth or falsity of the subject's statements, based on the changes in those responses. Similarly, the Brain Electrical Activation Profile (BEAP) test measures responses within the brain, in order to ascertain whether or not the subject has recognised the stimuli to which they have been exposed.

In court, the appellants claimed that the involuntary administration of these tests violated the accused persons' rights against self-incrimination (under A.20(3)) and their personal liberty (under A.21). Thus, what the case rested on was whether recording physical stimuli (in response to the tests) amounted to compelling a person to be a "witness against himself".

The court interpreted Art. 20(3) to be protecting 2 key features of an investigative process:[99]

> 1) *ensuring reliability of the statements made by the accused, and*
>
> 2) *disincentivizing the use of interrogation tactics that violate the **dignity and bodily integrity** of the person being examined. Here, it serves as a check on police behaviour and a safeguard against torture and other `third-degree methods' that could be used to elicit information.*

### Testimonial compulsion

Following the Kathi Kalu court's precedent, the Supreme Court examined whether the use of these techniques involved "testimonial" compulsion that would be covered by Article 20(3). For this, it would be a testimonial act if it involved "*the imparting of knowledge by a person who has personal knowledge of the facts that are in issue*."

**99** Paras 91, 92

The court held that the use of these techniques *was* testimonial evidence because

> *"By making inferences from the results of these tests, the examiner is able to derive knowledge from the subject's mind which otherwise would not have become available to the investigators. These two tests are different from medical examination and the analysis of bodily substances such as blood, semen and hair samples, since the test subject's physiological responses are directly correlated to mental faculties. Through lie-detection or gauging a subject's familiarity with the stimuli, personal knowledge is conveyed in respect of a relevant fact."*[100]

Additionally, the court also made a series of observations about the importance of the privacy of "mental processes;" while much of criminal law allows state interference into physical privacy, such as that of the body and physical spaces through arrests, detention, search and seizure orders etc, the court observed that it cannot extend to compelling a person to imparty personal knowledge.

*"Forcible interference with a person's mental processes is not provided for under any statute and it most certainly comes into conflict with the right against self-incrimination."*[101]

In this judgement, the court also expanded on the definition of "accused of an offence." They held that this term covered a wide ambit that included people formally charged with offences, as well as people whose answers *could* expose them to criminal charges.[102]

## *Ritesh Sinha v. State of UP*

In 2019, the Supreme Court determined the constitutionality of compelling voice samples from accused persons during the course of an investigation, in the absence of any legal provisions that allowed for it. The investigative agency in question wanted to confirm the identity of the accused in a phone conversation they had acquired.

Applying the Supreme Court's judgement in *Kathi Kalu Oghad*, the court held that voice samples are similar in nature to finger prints, palm prints etc, and would therefore trigger Article 20(3) protections.

## *Virendra Khanna v. State of Karnataka and Anr*

In 2021, the Karnataka High Court delivered its judgement in *Virendra Khanna v State of Karnataka*. The case called for the High Court to decide on the validity of a trial court order that had asked the petitioner to provide passwords to their smartphone and email account to the investigative agency. This was the result of two applications by the police before the court, the first asking for the petitioner to provide access to his phone and accounts, and

**100** Paragraph 160

**101** Paragraphs 190-193

**102** Para 109

when he complied with that order, asking for directions that the Petitioner be subjected to a polygraph test to confirm the mobile / email passwords, as it appeared that the Petitioner had been lying about the same during investigation. The court allowed this application as well and directed the polygraph tests be conducted. The Petitioner challenged this order and the consequent direction to undergo a polygraph test This case was also decided on issues of Article 20 right against self incrimination, and Article 21 personal liberty and privacy.

**Right against self-incrimination**

The High Court held that compelling an individual to produce the password for their mobile phone and for their email account would not be self-incriminating, as providing a password did not disclose anything incriminating, and was not the "testimonial compulsion" which Article 20(3) sought to protect. The court found that such passwords were not, in fact, a personal testimony, but 'physical evidence', akin to fingerprints, blood samples or handwriting samples. Accordingly, the mere production of a password would not be testimonial compulsion, and would be allowed.

**Right to privacy**

The High Court knew about the possible violation of the right to privacy due to the immense amounts of data available on digital devices. It noted that once a law enforcement agency has access to a device, the person's entire life is accessible. However after stating the same, the court changed its course by saying use of such information would not violate the right to privacy as it was covered by exemptions. In the same breath, it mentioned that unlawfully disclosing such data with third parties could invite penalties.

While a criminal investigation does require some degree of compromise on individual privacy, allowing all activities in the context of an investigation does away with the protection afforded by the fundamental right. As per this precedent, the police seem to have unrestrained access to an individual's personal devices. The court did not formulate any safeguards against this snooping, nor did it establish a time limit for this practice. .

Finally, the case did not lay down any remedies for such a violation of the right to privacy. Even though the HC noted that third party disclosures could lead to a breach, there is nothing more that they offered in the judgement.

Further, the following issues were before the court:

1) Can a direction be issued to an accused to furnish the password, passcode or Biometrics in order to open the smartphone and/or email account?

The Court in response said - During the course of the investigation, the officer can always make a direction/ request to furnish certain information. These directions are routine in any investigation. Thus, an investigation officer can direct/request to furnish a password to access an electronic device. However, it is up to the accused to accede to the said request or direction.

2) Can a Court issue a suo moto order to the accused to furnish a password, passcode or Biometrics?

The Court in Response said - The court by itself cannot issue a *suo moto* order for furnishing of the password, passcode, or Biometrics. The Court is not part of the investigation. The Court can only act on an application being filed by either of the parties.

3) In the event of a direction being issued and the accused not furnishing the password, passcode or Biometrics, what is the recourse available to an Investigating Officer?

The Court in Response said - In the event of the accused not providing the password, passcode or Biometrics, the Investigating Officer can approach the Court seeking necessary directions to the accused to provide the same and/or carry out a search of the smartphone or any electronic equipment. The Investigating Officer could approach the concerned Court seeking for issuance of a search warrant to carry out a search of the smartphone and/or electronic equipment.

4) What is the consideration for the issuance of a search warrant in order to search a smartphone or computer system?

The court in response said - The court observed that there are no specific provisions in the CrPC or Information Technology Act that provide for the search of an electronic device like a smartphone, laptop etc. Therefore, reliance will have to be placed on the existing provisions. It was held that sections in the CrPC dealing with summons and search and seizure become relevant. Section 93 and 100 provide for the search of any *premises or the like*. Section 93 confers power on certain courts to issue search warrants, on a person not willing to produce a document or a thing as directed under Section 91 of Cr.P.C, or where the document or thing is not known to be in possession of any person or, Where the Court considers that for the purpose of any inquiry, trial or other proceedings, a general search or inspection would serve the purpose. Section 100 provides for the search of a closed place by directing any person in charge of that place to make it accessible. Based on these, the provisions court held that a search warrant to search an electronic device can be granted.

The court held that in case of an emergency situation it cannot be expected of the Investigating officer to rush to a court of Law to obtain a warrant, such a requirement would amount to negating their powers and impinging on their functions. Thus if an emergency search is made, there must be recorded in writing made by the investigating officer, specifying in writing as far as possible the reasons for conducting such a search without a warrant.

5) Would the data gathered from a smartphone and/or email account *ipso facto* prove the guilt of the accused?

The Court held NO, the data so gathered is not ipso facto proof of guilt of the accused. It is like any other document obtained during the course of the

investigation. The data gathered would have to be proved during the course of the trial as done in any other matter.

6) Would providing a password, passcode or Biometrics amount to self-incrimination or testimonial compulsion?

The  Court held that NO, providing password to an electronic device does not amount to self-incrimination. This was based on the reason that providing a password only provides access to a device. Which means it only provides access to data/ information stored in the device. It is not a testimony. The court relied on *Kathi Kalu Oghad*, where it was held that providing fingerprints or writing samples does not amount to testimony. The reasoning was that after receiving the fingerprint the police has to do a further analysis to establish or prove something, the information in itself does not prove anything. This same logic was applied by the court in the instance of password. After getting the password the information that is accessed by the Police has to be proved by using the rules of evidence. Password in itself does not prove anything.

7) Would providing of password, passcode or Biometrics violate the right to privacy of a person providing the said password, passcode or Biometrics?

The court held that it will not be a breach of privacy of a person as this falls under the exceptions carved out in Puttaswamy Case. However, the disclosure, making public or otherwise in court proceedings would have to be determined by the concerned judge by passing a judicial order. In no case could such details or data be provided by the investigating officer to any third party during the course of investigation without the written permission of the court seized of the matter. The responsibility of safeguarding the information or data which could impinge on the privacy of the person will always be that of the investigating officer, if the same is found to have been furnished to any third party the investigation officer would be proceeded against for dereliction of duty or such other delinquency as provided.

8) What steps could be taken if the accused or any other person connected with the investigation were to refuse to furnish a password, passcode or Biometrics despite issuance of a search warrant and or a direction to provide a password, passcode or Biometrics of that person?

The person is to be given only one opportunity to provide the password. If they do not provide it, or provide incorrect passwords then an adverse inference can be drawn towards them. In addition to that, the investigating officer can then use any other method to access the phone, this method cannot be challenged by the person at any stage.

## *P. Gopalakrishnan alias Dileep v State of Kerala*

In this case, petitioners argued that the notice issued by the police asking for the petitioners to submit their mobile phones for the investigation violated Art 20(3). The court however

relied on the judgement in *Kathu Kalu Oghad* and *Virendra Khanna* to hold that giving access to mobile phones does not amount to "self-incrimination" as protected by the Constitution.

The Kerala HC bench found compelling the Supreme Court's judgement on what amounted to being "a witness," as well as Karnataka HC's holding in Virendra Khana that data accessed by an investigative agency through devices is only in the nature of "documents and information," and does not in any way amount to testimony.

## *CBI V. Mahesh Sharma and others*[103]

The court in this case went into the provisions related to the statutory powers of an investigating agency. The court in this case held that the password for a computer system falls under the category of testimonial fact as it furnishes a link in the chain of evidence. The court also said a password by itself is not a self incriminating testimony but the password is used to access data which is stored in an electronic device which is seized. Further the court has observed that it is not bound by ***Virendra Khanna*** because of territorial jurisdiction of Karnataka High Court.

## *Vijay Madanlal Choudhary v. Union of India*[104]

Over the last fifteen years, the SC has received a large number of cases, including writ petitions, appeals, and requests for special leave against challenges to the constitutionality of some PMLA provisions. A few resulted from decisions made by higher courts or lower courts that denied requests for bail, discharge, quashing, etc. The Supreme Court limited itself to providing answers to legal concerns that contested the PMLA's provisions, without going into the factual details of each case that was included in the batch of matters. The following discusses the arguments made against the PMLA's provisions as well as the SC's ruling.[105]

The premise of the petition was that the Prevention of Money Laundering Act is being used against the legal process outlined in the CrPC. The safeguards put in place for the search and seizure of assets and vessels during ED raids—which allowed for the search and seizure to occur without the filing of a formal complaint and the making of arrests without a warrant—have been weakened by revisions made over time.

The Court considered several act provisions that were contested and determined that, as PMLA is a Special Law, it supersedes the standards set forth by the CrPC and, as such, cannot be shown to be in violation of the accused's fundamental rights and the principles of natural justice.

**103** https://www.livelaw.in/pdf_upload/displayphp-442128.pdf

**104** https://indiankanoon.org/doc/14485072/

**105** https://www.mondaq.com/india/money-laundering/1262376/explainer-%7C-vijay-madanlal-choudhary-and-others-v-union-of-india-and-others

The Supreme Court ruled that the PMLA's provisions for the search and seizure of property and the search of individuals have built-in safeguards. These safeguards include requiring high-ranking officials to exercise their power only and requiring them to adhere to procedures that ensure fairness, accountability, and transparency throughout the entire search and seizure process. This is not the same as the clause included in the Code of Criminal Procedure, 1973 ("CrPC"), which permits any police officer to proceed simply on the basis of a predicate offence allegation or suspect. Furthermore, the PMLA's procedures for searches and seizures are intended to prevent money laundering in addition to looking into alleged money laundering crimes.

## *Ram Ramaswamy and Ors. v. Union of India and Ors*

In early 2021, five academics submitted a plea asking for the creation of guidelines to regulate the police and investigating agencies on seizure of mobile phones and computers of the academia as "electronic evidence" by investigating agencies during raids, saying they have a right to protect their work and research embedded in these personal digital devices.[106] Claiming that devices of several people from the academic field have been seized by investigating agencies in the recent past, the petition stated that it causes loss of research work. The lack of any procedures for the police for appropriate mode of recovery of material in the electronic or digital format, which is unique only to digital devices, threatens the damage or loss of such work.

In 2022, the Foundation for Media Professionals ('FMP') approached the Supreme Court seeking regulation of the police's power to search or seize electronic devices.[107] In October, the Court issued notice to the government to respond.[108] The petitioners have asked the government for the following things:[109] Both matters are tagged currently.

> 1) The Law enforcement agencies should obtain a warrant before searching devices. The warrant should not be general, and it should set out the information the police expect to find on the device, with reasonable cause for such expectation. If there isn't a warrant, the search should be deemed as unconstitutional.
>
> 2) An application for a warrant should demonstrate to the magistrate that it fulfils the standard of proportionality under Article 21, which means 1) obtaining evidence should be impossible by other means; and 2) state interests justify the highest degree of violation of privacy.

**106** https://scroll.in/latest/990961/sc-issues-notice-to-centre-on-academics-plea-seeking-guidelines-on-seizure-of-electronic-devices

**107** https://internetfreedom.in/sc-issues-notice-in-fmp-petition-regulation-of-polices-power-to-search-devices/

**108** https://www.medianama.com/2022/10/223-stop-police-search-mobile-phones-plea-in-sc/

**109** https://drive.google.com/file/d/1HoZuNGM6pkAePSayDXMucHZy_1wAnbBE/view

3) Law enforcement agencies should put in place safeguards to ensure that the information they obtain is not leaked and that it's deleted once no longer necessary for the investigation. Further, information should not be shared with other government agencies.

A notice was issued on the petition and in the last hearing, the Supreme Court has asked the Union to frame guidelines for search and seizure.

## Safeguards per the existing laws

Search and Seizure per the trends and the cases observed can take place under a variety of provisions such as UAPA, PMLA, the Income TaX act and even under regular investigation. News reports have brought to line how police personnel in Hyderabad were searching mobile phones as part of their crackdown on drugs.[110]

In absence of concrete law and framed guidelines these are the following safeguards that can be used by citizens in respect to search and seizure of devices.

A person must look for following elements in a search warrant: [*absence of these makes a search illegal, which means a person can resist the police from entering their premises*]

i) Name and the designation of the officer must be specified.

ii) The place where search is to be conducted must be specified.

iii) Documents or thing which is to be searched must be distinctly specified (unless a general warrant)

iv) seal of the court

In the case of *Siddanna v. State of Mysore*, *AIR 1966 Mys 289* it was held that if the warrant is not issued in the proper format as provided in the code, the search will become illegal.

The safeguards that were provided in the *Virendra Khanna* judgement are the following:

In the case of a personal computer or a laptop:

1) When carrying out a search of a premises in relation to an electronic device the search team must be accompanied by a Forensic Examiner.

2) The police officer himself cannot conduct the search of an electronic device. It must be done by an authorised and qualified person like a forensic examiner.

3) While conducting the search, photographs must be clicked of the place where such a device is kept so that all connections of wires can be seen and also of back and

110 https://www.hindustantimes.com/india-news/hyderabad-cops-criticised-for-checking-mobile-phones-as-part-of-crackdown-on-narcotics-101635420049868.html

front, to see all the connected peripherals. A diagram showing the manner in which the computer is connected should also be prepared.

4) If a computer is switched off, it should not be switched on. If it is switched on, then it should not be switched off. The investigating officer should try to get the services of a forensic examiner to safely download the data (on RAM and network data) before switching off.

5) If it is switched on and the screen is black, mouse can be moved and when the screen appears a picture of the screen must be clicked.

6) MAC address should be identified and secured.

7) In case a Forensic examiner is not available then the computer should be disconnected and then packed in faraday covers. Computer and wires are to be packed separately and labelled.

8) In case of a laptop if removal of power cord does not shut it down then battery can be removed. In case that also doesn't work then shut it down normally and store in a faraday bag.

*Seizure of networked devices:*

1) The investigating officer is to ascertain if the electronic device is connected to any remote storage devices or shared network devices. In case it is, the officer is to seize those too.

2) The officer has to seize any wireless access points, routers, modems, and any equipment connected to such access points, routers, modems which may sometimes be hidden.

3) The officer has to find out if there are any unsecured wireless networks that can be accessed from the location of the device. If any are found then the officer must secure them as the accused might have used them.

4) Find out who is maintaining and running the network. Then obtain network logs of the device that has to be searched or seized.

*Mobile devices:*

In the Court held that mobile devices would mean and include smartphones, mobile phones, tablets, GPS units, etc. It provided some additional safeguards:

1) The device must be packed in a faraday bag so that it does not receive any wireless communication. Sim card should also be removed and packed in a separate faraday bag.

2) Keep it recharged so that the phone does not shut down, as that will result in loss of data in the volatile memory.

3) If the mobile is already switched off then the battery could be removed and kept separately.

4) In case it is switched on, put the phone in airplane mode.

*General:*

1) Keep the device in a dust free and temperature controlled environment.

2) If the investigating officer seizes any external storage device it must be stored and labelled separately in a faraday bag.

3) The devices are to be kept away from magnets, radio transmitters etc.

4) While conducting a search police can keep the instruction manuals related to the device and also look for written passwords and obtain the same.

5) Everything related to this process must be written down properly by the officer.

## Conclusion

In an ongoing case against the founder of Gaincoin, Ajay Bharadwaj, charged with counts of crypto currency scam, the Supreme Court asked the accused to provide password and username details for his crypto wallet with the Enforcement Directorate for the purpose of carrying out proper investigation. The order was brief, and did not come with any direction as to how this data would be handled, and its implications on the constitutional guarantees of the right against self-incrimination and right of privacy.[111]

The Supreme Court of the United States in Riley V. California (573 U.S. 373 (2014) dealt with the warrantless search of a cell phone. The Court in this judgement said that there were differences between mobile phones and other seized objects obtained from an arrested person. It further said that there is a huge amount of highly sensitive data that is stored in a mobile phone and a warrantless search would violate the 4th Amendment.[112]

**111** https://indiankanoon.org/doc/116795780/

**112** https://privacylibrary.ccgnlud.org/case/riley-vs-california

# Internet Shutdowns

Internet shutdowns have long been used in India, by both national and state governments, to restrict communication during times of crisis. These crises, however, range from the threat of terrorist organisations to cheating during examinations.[113] Through 2018 to 2022, India topped the list for the most number of internet shutdowns in the world.[114] A study conducted in ten countries where Internet disruptions and restrictions were recorded showed that in the first half of 2022, India alone accounted for 85% of the internet shutdowns.[115]

## Background

The Indian government implements internet shutdowns across the country through the operation of two legislative frameworks, by section 144 of the Code of Criminal Procedure and under section 5(2) of the Telegraph Act and the Suspension Rules. Different executive authorities are allowed the power and discretion to institute a shutdown under these laws, although the grounds triggering a shutdown are vague and open to interpretation. The manner in which shutdowns take place have also changed drastically in the last couple of years. There have been instances of partial shutdowns, where just social media has been banned or the internet has been shut down only for a particular period of time. In Sambalpur, in Orissa for example internet was shutdown between 7AM-7PM.[116] The state of Manipur has had a shutdown for over 200 days.[117] There have been orders which have imposed shutdown only for mobile internet users whereas broadband users can access the internet in a limited capacity. This shows the changing nature of internet shutdowns. There have also been consultation papers released by different government authorities asking for selective banning of the internet.

It is to be noted that Criminal Laws in India have been replaced with new acts which will come in effect from 1st July 2024. Internet shutdowns are imposed using some provisions of the

**113** https://edition.cnn.com/2021/09/28/tech/india-rajasthan-reet-exam-internet-shutdown-intl-hnk/index.html; https://www.indiatimes.com/news/india/internet-assam-shut-cheating-exam-577737.html; https://www.thequint.com/voices/opinion/calcutta-hc-pushes-back-normalisation-internet-shutdowns-india-unreasonable-disproportionate#read-more

**114** Access Now Report, https://internetshutdowns.in/

**115** https://www.techcircle.in/2022/08/04/india-accounts-for-most-internet-shutdown-cases-in-the-world-in-2022-report

**116** https://www.newindianexpress.com/states/odisha/2023/apr/21/sambalpur-violence-internet-respite-but-mobile-users-continue-to-wait-2568001.html

**117** https://www.thehindu.com/news/national/other-states/mobile-internet-ban-in-manipur-extended-till-nov-8/article67503273.ece

Criminal Codes as well as Telecom Acts. It is yet to be seen the manner in which these acts will be implemented as rules are yet to be implemented.

### *Section 144, CrPC*

Prior to 2017, internet shutdowns in India were predominantly issued under section 144 of the CrPC.[118] Section 144 empowered an authorised official (including a District Magistrate or a sub-divisional magistrate) to issue an order, if they are convinced there is i) sufficient ground, ii) need for immediate prevention, iii) to prevent obstruction, annoyance or injury to any person lawfully employed, etc. Once these grounds are established, the official can direct any person to abstain from a certain act or to take certain order with respect to certain property in their possession/management.

Section 144 remains untouched in the new Criminal laws as well.[119]

A bare reading of the elements of this provision makes it clear that section 144 does not provide any direct, explicit source of power for governments to order internet shutdowns. Accordingly, District Magistrates interpreted this section to mean that their 'sole opinion' allowed them to direct telecom service providers to disrupt services.[120] Orders passed under this provision were ex-parte, and the absence of any mechanisms to review such orders, exacerbated the entrenched discretion of the authorised officials.[121]

## The Temporary Suspension of Telecom Services Rules ("Suspension Rules")

Section 5(2) of the Indian Telegraph Act of 1885 allows for the government to stop "*telegraphic transmission*" in times of public emergency or in the interest of public safety.[122] The phrase "*telegraphic transmission*" is broadly defined, and can include access to the internet as well.[123]

The Suspension Rules creates a procedure for the government to exercise this aforementioned power under section 5(2) of the Telegraph Act, when it comes to internet services. The Rules empower either (a) to the Secretary to the Home Ministry in the case of the Central Government, and (b) to the Secretary to the Home Department, in the case of the State Government to suspend internet services; Rule 2 explicitly mentions that such suspension of services can only be effectuated by these authorities.[124]

**118** https://sflc.in/legality-internet-shutdowns-under-section-144-crpc

**119** https://www.deccanherald.com/opinion/bharatiya-nagarik-suraksha-sanhita-no-decolonisation-here-2675972

**120** https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3254857

**121** Id

**122** Indian Telegraph Act, 1885

**123** https://cis-india.org/internet-governance/blog/india-digital-freedoms-2-internet-shutdowns

**124** Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017

The Rules also prescribe a Review Committee, that is responsible for examining whether an internet shutdown complies with Section 5(2). In 2020, the Indian government inserted an amendment to the Rules which restricted the maximum number of days that an internet shutdown can be ordered for, to be fifteen days.[125]

## The Telecom Act, 2023

The Telecom Act, 2023 replaced the Indian Telegraph Act, 1885, the Indian Wireless Telegraphy Act, 1933, and the Telegraph Wires (Unlawful Possession) Act, 1950. The act will be bound to come into implementation at a later date which has not been notified yet. The act has sparked controversies on different lines - manner of its passage as well the provisions in place.

The provisions around Internet Shutdowns state that In the interest of public safety or sovereignty, the Central Government, State Governments, or authorised officers may suspend telecommunication services, or certain kinds of services, according to Section 20(2)(b) of the Act. The Act itself does not provide detailed rules for this broad jurisdiction, which is intended to enable required acts during emergencies or to protect public safety. Instead, the specifics will be outlined in subsequent Rules. The rules are yet to be notified. This lack of notified rules prompts worries about possible abuse or capricious use of this authority, which can result in a rise in the reactive suspension of telecom services.

Article 19(1)(a) of the Indian Constitution guarantees the right to freedom of speech and expression, which is violated by the suspension of communications services. Furthermore, the Act's modifications to the TRAI Act may change how telecommunications services are regulated throughout the nation, possibly calling for TRAI to have a bigger role in supervising these suspensions.

The Supreme Court's decision in Anuradha Bhasin v. Union of India (2020), which established the guidelines that internet service suspensions are harsh measures which must comply with the necessity and proportionality standards. The Court outlined procedural protections, including the posting of suspension orders online and regular reviews. Some states have not complied with these guidelines in suspending internet services. It is to be seen whether the rules notified under the act will incorporate the guidelines laid down by the Supreme Court in Anuradha Bhasin v. Union of India or not.

## Consultation Paper on The Regulation Mechanism for OTT communication services and the Selective Banning of OTT services

In July 2023, a consultation paper on the Regulation Mechanism for Over-The-Top (OTT) Communication Services and the Selective Banning of OTT Services was launched by the

125 https://internetfreedom.in/telecom-suspension-rules-amendment-15-day-time-limit/

Telecom Regulatory Authority of India. The paper's release reflected the belief that new and appropriate rules for OTT regulation in the nation must be framed through a new consultation process. Currently OTT's are regulated under the Information Technology act as well as the Indian Telegraph Act. The consultation paper seeks to explore the idea that selectively banning certain OTT services will prevent law and order situations during public unrest situations. This means that only certain OTT services will be banned during public emergencies as opposed to the entirety of the internet. Selectively banning internet services through TRAI is out of the ambit of the regulatory powers of TRAI but rather rests under the IT act. In addition, there is no conclusive proof that shutting down the internet can prevent public order situations.

## Freedom of expression and internet shutdowns

Article 19(1)(a) protects citizens' rights to free speech and expression, except in certain specified situations. Internet shutdowns are undoubtedly a violation of this speech. First, the internet has become a vital medium for speech and expression, and a restriction on the medium is a restriction on the right itself.[126] Second, the freedom of speech and expression has been consistently interpreted by the Supreme Court as including the right to information, which is undoubtedly affected by internet shutdowns. Thus, the constitutional validity of shutdowns are tested against the following:

1) The restriction should be imposed by "law".

2) It should be in pursuance of one of the nine standards listed in Article 19(2).

3) It should be "reasonable"

## Judicial cases

### *Gaurav Vyas v. State of Gujarat*

In 2015, Gujarat witnessed mass agitations by the Patidar community asking for reservations in public sector jobs and education.[127] The state government imposed a mobile phone internet shutdown in some parts of the state to take control of the law and order situation.[128] The shutdown lasted about a week, with differential access in different parts of the state.[129]

**126** This was held in Anuradha Bhasin v Union of India (2020) 3 SCC 637 : 2020 SCC OnLine SC.

**127** Nidhi Sinha, 'Patel Agitation Turns Gujarat into a Battlefield' (LiveMint, August 27 2015),

**128** Mugdha Variyar, 'Gujarat Bandh: WhatsApp and Mobile Internet Suspended as Hardik Patel Rally Turns Violent' (International Business Times, 26 August 2015)

**129** Express News Service, 'Mobile Internet Ban Ends; Ahmedabad, Surat Last Out' (The Indian Express, 2 September 2015)

In this backdrop, law student Gaurav Vyas filed a public interest litigation in the Gujarat High Court arguing that the shutdowns were unconstitutional.[130]

The petition argued that:[131]

> a) The applicable law for an internet shutdown is Section 69A of the Information Technology Act, 2000 ("IT Act") and not Section 144 of the CrPC which had been resorted to by the state government.
>
> b) A total mobile phone internet ban is not narrowly tailored, as blocking only social media websites could have achieved the needed outcome.

In response to the first argument, the Court held that the fields of operation of the two provisions were different. According to the Court,

> *"Section 69A may in a given case also be exercised for blocking certain websites, whereas under Section 144 of the Code, directions may be issued to certain persons who may be the source for extending the facility of Internet access."*[132]

As for the claim that the internet shutdown was overbroad, the court rejected it, citing two reasons:

> *"...one is that normally, it should be left to the authority to find out its own mechanism for controlling the situation and the second is that there are number of social media sites which may not be required to be blocked independently or completely. But if Internet access through mobiles is blocked by issuing directions to the mobile companies, such may possibly be more effective approach found by the competent authority."*[133]

In this case, the court did not seem very concerned about the implications of the mobile internet ban on citizens' rights to free expression, livelihood or access to information. It also considered the ban minimal, because "access to Internet through broadband and wi-fi facility was permitted (or rather was not blocked)."[134]

In February 2016, Gaurav Vyas filed a special leave petition ("SLP") in the Supreme Court against the High Court's judgement.[135] However, a two-judge bench of the Supreme Court dismissed the SLP at the admission stage itself, making final the High Court judgement.

**130** Gaurav Sureshbhai Vyas v State of Gujarat, 2015 SCC OnLine Guj 6491.

**131** Id

**132** Gaurav Sureshbhai Vyas v State of Gujarat, 2015 SCC OnLine Guj 6491 [9].

**133** Gaurav Sureshbhai Vyas v State of Gujarat, 2015 SCC OnLine Guj 6491 [11].

**134** Gaurav Sureshbhai Vyas v State of Gujarat, 2015 SCC OnLine Guj 6491 [11].

**135** Gaurav Sureshbhai Vyas v State of Gujarat, 2016 SCC OnLine SC 1866

## *Paojel Chaoba v. State of Manipur*

In 2018, internet services were suspended in Manipur, in response to protests that started following the suspension of the Vice Chancellor of Manipur university on allegations of financial irregularities.[136] Initially, the suspension was for 5 days,[137] but within a month of resumption of services a second order suspended it for 6 days.[138] These orders were challenged in the Manipur High Court.

This case is important, as it held that the state's measure was overbroad in its application. Relying on the testimony of a system analyst and a computer programmer who found it "technically feasible" to selectively block only certain internet applications "without disturbing the entire mobile internet as a whole,"[139] the court rejected the state's claims. Observing that internet services had become an important part of a daily citizen's life, it held that seeking to prevent use of social media networks on mobile phones was not enough of a reason to cause the inconvenience of suspending mobile internet access.[140] The court asked the Government of Manipur to consider blocking only social media applications WhatsApp and Facebook, as opposed to suspending mobile internet services in entirety. However the petition was eventually disposed of because internet services had resumed.

## *Banashree Gogoi v. Union of India*

In late 2019, widespread protests began against the Citizenship Amendment Bill, 2019. In December, the government invoked the Suspension Rules[141] and issued daily notifications to suspend internet services in the state. In response to public interest petitions filed, the Gauhati high court noted no incidents of violence or public disorder had occurred in several days, and passed an order asking the state government to disclose "*the entire material that weighed with the respondents in continuing suspension of internet/mobile data service*."[142]

The state government responded with an affidavit stating that a review meeting of state authorities had taken place, and they decided to continue the shutdown based on intelligence information they were receiving.[143] They also put on record a message from the director of

**136** Prasanta Mazumdar, 'Manipur University Vice Chancellor Placed under Suspension by President' (The New Indian Express 18 September 2018)

**137** 'Manipur Suspends Internet Services for 5 Days over MUSU Strike' ( India Today, 21 June 2018) https://www.indiatoday.in/india/story/manipur-suspends-internet-services-for-5-days-over-musu-strike-1292293-2018-07-21).

**138** Trisha Jalan, 'Internet Shutdown: Mobile Internet Suspended for 6 Days in Manipur' (MediaNama, 24th September 2018)

**139** Aribam Dhananjoy Sharma v State of Manipur, PIL No. 47 of 2018, decided on 17th November 2018, 8

**140** Id, 7

**141** Temporary Suspension of Telecom Services Rules (Public Emergency or Public Safety) Rules, 2017

**142** Banashree Gogoi v Union of India 2019 SCC OnLine Gau 5584, paragraph 4

**143** Id, 5.

the intelligence bureau, that was for the court's perusal only, which was "*in the nature of an advisory to alert the officers and to marshal their resources and ensure maintenance of law and order in their areas as intensification of protests is anticipated and the scale of protest programmes may increase in the days to come*."[144] It was on the basis of this advisory that the government chose to continue the shutdown.

The court, in response, noted the significance of the internet in everyday lives, and the impact of its suspension. Reminding the state that internet shutdowns must only be imposed out of necessity, it stated

> "*Very importantly, no material is placed by the State to demonstrate and satisfy this Court that there exists, as on date, disruptions on the life of the citizens of the State with incidents of violence or deteriorating law and order situation which would not permit relaxation of mobile internet services*."[145]

The court ordered the State of Assam to restore internet connectivity immediately,[146] because "the period of acute public emergency which had necessitated suspension of mobile internet services" had diminished[147], and the state was unable to effectively show why it was necessary any longer. Applying the principle of proportionality, the court challenged the government's claim on the necessity of a continuing internet shutdown, and did not simply defer to the government's own assessment of the situation.

## *Anuradha Bhasin v. Union of India*

In 2019, following crucial amendments made to Article 370 of the Constitution of India (that removed the special status given to the State of Jammu and Kashmir), the central government suspended all modes of communication in the state, including the internet. In October of 2019, the government reinstated landline and mobile services, but continued to suspend internet services. A challenge was brought before the Supreme Court, and continued to operate largely on the question of internet shutdowns and their interplay with freedom of trade and speech.

### Fundamental right to internet

This case first set out to establish whether the Constitution of India guarantees a fundamental right to the internet. The court agreed that the freedom of speech and expression included the right to "disseminate information to as wide a section of the population as is possible."[148] Noting the value of the internet in recent times, both for sharing information and in trade and

144 Id, 5.

145 Id, 7

146 Id, 10

147 Id, 8.

148 Anuradha Bhasin v Union of India (2020) 3 SCC 637 : 2020 SCC OnLine SC 25, 28.

commerce[149], the court held that the right to express freedom of speech through the medium of the internet was protected under Article 19(1)(a).[150]

**Suspension Orders**

In court, the unavailability of the suspension orders became an issue, when the respondents admitted that they could not produce them as "the orders were being withdrawn and modified on a day-to-day basis."[151]

The court held, however, that the government was obligated to place all its suspension orders on record. For the petitioner to be able to make a case, they had to have all the information, especially when it is in the sole possession of the state.[152] Additionally, rights available to citizens under Article 19(1) also include the right to information, entitling them to see these orders.[153] Thus, the court held that the government must take proactive steps to produce orders when they are challenged for fundamental rights violations, and cannot claim "difficulty" in producing them as valid grounds.[154]

**Reasonableness**

For a long time, the serious security and terrorism issues that plague Jammu and Kashmir have been used as justifications for many government measures that interfered with citizens' fundamental rights. In this case, The court sought to answer the question of whether there existed a clear and present danger that justifies the restriction.[155] It noted several factors in making this decision: "the territorial extent of the restriction, the stage of emergency, nature of urgency, duration of such restrictive measures and nature of such restriction."[156] Applying these, the court held that the state could only impose a shutdown during the stage of emergency, when it is "necessary" and "unavoidable" to do so, and no "less intrusive remedy" exists.[157] During this, the state must also explore the alternative option of blocking only social media websites instead of the entire internet.[158]

The court also noted that these shutdown orders must be only for a specified duration, and that indefinite orders were not permissible. Since this was not mandated by the Suspension

**149** Id, 25, 30.

**150** Id, 27 to 29.

**151** Id, 15

**152** Id, 75

**153** Id, 11.

**154** Id, 20, 21.

**155** Id, 38

**156** Id, 79

**157** Id, 108.

**158** Id., 111

Rules, the court recommended that the legislature fill this gap[159], and in the meanwhile directed the Review Committee, constituted under the Rules, to conduct a periodic review of the suspension order every seven days.[160] For this, the Committee was tasked with checking if the suspension complied with the requirements contained in Section 5(2) the Telegraph Act, and it was proportionate and necessary.[161]

Finally, the court directed the government to:[162]

> 1) publish all orders passed under Section 144 of the CrPC, and those suspending telecom or internet services.
>
> 2) Any order suspending internet services indefinitely is impermissible under the Suspension Rules.
>
> 3) All suspension orders must be well reasoned, adhere to principles of proportionality, and must not extend past necessary duration.
>
> 4) Until further amendment of the Suspension rules, the review committee constituted under the rules must conduct a review of current orders every seven days.
>
> 5) To review all suspension orders currently in force, and revoke those contrary to the judgement.

Despite these favourable orders, the court did not actually strike down the suspension orders challenged in the case, leaving it to the judgement of the government (or more specifically, the Review Committee).

## *Foundation for Media Professionals v. Union Territory of J&K*

Following the continued restriction of internet services in Jammu and Kashmir to only 2G bandwidth (while the rest of the country used up to 4G), the Foundation for Media Professionals filed a petition before the Supreme Court praying for 4G services to be restored immediately.[163] Since this was during the Covid-19 pandemic, the petition claimed important fundamental rights apart from that of free speech, including rights to health, access to education, access to justice, and trade and livelihood.[164] Following the Anuradha Bhasin judgement, the petition also claimed that the restriction on 4G internet during the pandemic was a disproportionate measure, and violated other protections granted by the Anuradha court, such as the need for it to be the least intrusive measure, and for it being specifically

**159** Id, 108-109

**160** Id, 109.

**161** Id, 109.

**162** Id, 152

**163** Memorandum of Writ Petition, Foundation for Media Professionals v UT of J&K, (2020) 5 SCC 746.

**164** Id.

temporally limited.[165]

The court noted in its judgement that the suspension order "does not provide any reasons to reflect that all the districts of the Union Territory of Jammu and Kashmir require the imposition of such restrictions."[166] Nevertheless, a blanket order had been imposed throughout the state. Despite this clearly being in violation of the Anuradha Bhasin judgement, both in failing to give a reasoned order and in not limiting its scope, the court did not declare it unconstitutional. Instead, it referred to the prevalent militancy in the state, which was the only reason shared by the respondents to justify its measures, and held that while the petitioner's contentions would be upheld in normal circumstances, the prevailing terrorism in Jammu and Kashmir constituted "compelling circumstances" that "cannot be ignored."[167] Further, the court took into consideration the gradual steps taken by the government to lift these restrictions[168], and therefore did not find it necessary to interfere with the shutdown orders. Instead, it directed a "Special Committee" comprising the Union Home Secretary, the Union Communications Secretary, and the Chief Secretary of Jammu and Kashmir to "immediately" determine the necessity of the restrictions in place.[169]

## *Ashlesh Biradar v State of West Bengal*

Earlier in March, 2022, the state of West Bengal ordered for the suspension of internet for eight days, under section 144 of the CrPC, on the ostensible ground of preventing unlawful activities. However, as Internet Freedom Foundation (IFF) noted, the days for which the suspension was ordered, coincided with the date and time of secondary school examination in the state.[170]

This suspension order was challenged in the Kolkata High Court, and after extensive hearing, the court intervened in the ongoing shutdown, and stayed the order. The court found that the government did not have the lawful authority to issue an internet suspension order under section 144, nor did the order disclose why the internet needed to be suspended.[171]

This was a significant decision, since alongside the 2019 decision of *Banashree Gogoi v Union of India*, this was only the second time that any court had successfully intervened in an ongoing internet shutdown, and ordered the government to restore the internet.

**165** Id., 45-49.

**166** Foundation for Media Professionals v UT of J&K, (2020) 5 SCC 746, 16

**167** Id., 19.

**168** Id., 20.

**169** Id., 23

**170** https://internetfreedom.in/calcutta-hc-stays-internet-shutdown-issued-by-west-bengal-government/

**171** Id

### *Software Freedom Law Center, India V. State of Jharkhand*[172]

In a Public Interest Litigation (PIL), the Jharkhand High Court ordered the State Government to post on its website all prior orders regarding internet shutdowns and suspensions. The case involved a writ suit brought by the Software Freedom Law Center against the State Government of Jharkhand for repeatedly enforcing internet shutdown orders, in which the State Government also neglected to publish the order outlining the rationale behind the shutdowns. The court remarked that Respondents should have posted the order on their website, demonstrating the justifiable basis for the suspension order. The court also directed the state government to comply with the safeguards laid down in Anuradha Bhasin Judgement.

### *Aribam Dhananjoy Sharma, Paojel Chaoba & 2 Ors V. State of Manipur*[173]

The state of Manipur is undergoing an internet shutdown since 3rd May, 2023. After 2 weeks of the shutdown, a petition was moved in Manipur High court on May 3rd. Another petition was moved in the Supreme Court on the shutdown in Manipur but the apex court directed the petitioners to move to Manipur High Court (Chongtham Victor Singh & Anr. V. State of Manipur). The Manipur High Court granted limited reliefs to the petitioners, aggrieved by which the petitioners again moved to the Supreme Court. The apex court dismissed the petition of the petitioners.

## Conclusion

At the time of authoring this section, India has already seen 72 internet shutdowns[174], and given India's dubious distinction, it is anticipated that these numbers will only continue to go up in the coming days.

Nevertheless, persistent civil society advocacy, at both domestic and global levels, have resulted in some gains. Both the decisions of *Banashree Gogoi* and *Ashlesh Birdar* offer avenues of reform, and it is hoped that the precedents set by these decisions are followed by other courts who are confronted with similar situations in the future. Of notes is also the constitutional challenge to the TSTS Rules that is currently pending in front Gauhati high court[175], and the petition in front of the Supreme Court that challenges the states of Rajasthan, Arunachal Pradesh, West Bengal and Gujarat for suspending the internet to "prevent cheating" during exams.[176]

**172** https://globalfreedomofexpression.columbia.edu/cases/software-freedom-law-center-india-v-state-of-jharkhand/

**173** https://internetfreedom.in/60-days-manipur-internet-shutdown/

**174** https://internetshutdowns.in/

**175** https://internetfreedom.in/gauhati-hc-internet-shutdown-rules-update/

**176** https://www.forbes.com/sites/emmawoollacott/2022/09/13/indias-supreme-court-demands-clarity-on-internet-shutdowns/?sh=764bb96e108e

Given the precedence set by the past cases, as well as the overall incompatibility of internet shutdowns with international law standards[177], it is also hoped that these ongoing proceedings result in equitable decisions that respect an Indian citizen's right to freedom of speech and expression, which includes their right to receive and impart information.

177 https://www.icnl.org/wp-content/uploads/2.-Internet-Shutdowns-India-report.pdf

# Annexure 1

## Guide to effectively use Right to Information mechanism to obtain information

The right to information (RTI) is an important tool for advocacy worldwide. In authoritarian regimes, access to information is generally restricted or cut off, and the world has witnessed the weakening of Right to Information acts globally. In India the Right to Information is governed by the Right to Information Act, 2005. The answers obtained through these applications follow the back bones of several litigations, digital rights and otherwise. In order to obtain responses that can provide information in form of numbers, orders and other information it is pertinent that applicants follow the correct format and consider certain tips in mind.

1) List down requirements and attach proofs in form of news paper reports, screenshots wherever possible to substantiate the information seeked in the application. For example when seeking for an order on website blocking, ensure that a newspaper attachment is sent with your application. A reference for the same should be made in the application.

2) Before drafting the application, list down all the information that you need. Ensure that it is as objective as possible. Questions have to be specific and should not be blanket. For example, For an internet shutdown order, it can be asked whether a review committee was formed under Rule 5 of the Telcom Suspension Rules?

3) Address the application to the correct authority. Applications can get rejected if they are not addressed to the correct authority. There is some research that goes into finding the appropriate authority.

4) In cases where there is not surety on the correct authority that the application is supposed to go, mention in the application that 'If the information herein above is with any other public authority please transfer the application to such authority within a period of five days [as per S. 6(3) of the Right to Information Act, 2005] and inform me of such transfer and related communication'. This will ensure that the application gets transferred to the right authority.

5) Check whether the application can be filed online or offline. Check whether the department is there on the online portal. Many states have their individual state application portals. Doing a thorough research on whether a subject matter pertains to the state or the Center will help file the application in the correct place. For example, an application to seek order of website blocking has to be filed with the Center but an application to seek order for Internet shutdown will have to be filed with the state where the shutdown occurred.

6) The preference is to type out applications in a readable font. Handwritten

applications can be rejected on grounds of readability. Please mention your return address as well.

7) In most cases, one has to attach postal orders worth 10 rs INR with the applications. Different states accept payments in different ways. Please ensure to go through the state specific rules before filing the application and making payments.

8) Under the Right to Information Act, 2005, information is to be provided by the public authority within 30 days of receipt of application. There might be scenarios when information takes longer than that if the application has been transferred to another department. In such cases, the authorities have to send you an intimation that the application has been transferred. In cases where there is no intimation sent, one can appeal the application.

## Filing appeals and second appeals

1) In cases where the information provided by the Public Information Officer is insufficient or unsatisfactory or in cases where information is not provided within a period of 30 days, a first appeal can be filed. An appeal has to be addressed within a period of 30 days from receipt of it. In exceptional circumstances, this period can be extended to another 15 days.

2) A second appeal can be filed in case there is no response to the first appeal or the reply is unsatisfactory. This can be filed within 90 days of the receipt of response of the first appeal.

## Documents required to file First Appeals

First appeal lies with an officer who is higher in rank to the Public Information Officer. First Appeals can be filed under Section 19(1) of the RTI Act. The grounds for filing first appeals can be delay in response, insufficient information provided and denial of information. The details of the PIO can be obtained from the original response received. The first appeal should contain a brief statement of facts, this can include reference to the information sought, the response received, why the information received is insufficient or in correct and why the party is aggrieved. The first appeal should also mention the grounds of appeal. The application can also include a request for personal hearing in the appeal. A list of prayers or a single prayer should also be included in the appeal. The appeal should be signed. The general rule is that there is no fee to be paid for an appeal but in some states there is a fee applicable for filing appeals. The documents should contain the copy of the appeal application along with the reply which was received and any supporting documents. All of these should be self attested. Appeals should go through registered posts.


THE
CENTRE
FOR
internet
& society