DEEPSTRAT

STRATEGY . POLICY . ACTION

THEMES FOR DIGITAL INDIA BILL AN ANALYSIS

ONLINE HARMS AND RIGHTS

1. Research analysis

Summary of Recommendations:

1. Identify user harm for artificial and natural persons, vulnerable groups and map proportionate response and redressal mechanisms.

2. Identify scope of online harms not covered under existing legal provisions such as IPC and Competition Act. This would include damage to computer systems, tampering with computer source documents, etc.

4. Map out categories of actual and perceived harms to different age groups and across intermediaries. This should be done on the basis of evidence gathered on effects of online harms by Self-Regulatory Bodies (SRBs).

5. Platforms can develop mechanisms for users to control content they want to see and who they engage with.

6. Platforms can develop mechanisms to enforce age limits and age-checking measures for children.

7. Platforms can perform transparent risk assessment on measures taken to protect children from harm and also allow parents to monitor their online activities.

8. Platforms should publish annual accountability reports on the effectiveness of safety measures including metrics on prevalence of harmful content on platforms and user reports resolved.

9. SROs should be tasked with:

- Identifying relevant user harms for intermediaries
- Reviewing third-party audits of online safety measures taken by platforms.

Background

The Internet space has a lot of potential for driving India's economic development, but it is also fraught with challenges for user safety in terms of both psychological and financial harms. In order to create a safe and trusted space for an Internet user, the upcoming Digital India Act needs to address these user harms in a way that does not stifle innovation. Numerous international legislations contain provisions for regulation of online harms. Some of these provisions could be useful in the Indian context as well. This article provides recommendations on how the Digital India Act can tackle online harm in a way that boosts the digital economy and provides a trusted space for Internet users.

Introduction

Decades after the Internet came into existence, there is global recognition of the harms it poses to users. While the internet and internet-enabled technologies grew at a scorching pace, there has been a proportional rise in all kinds of harms that affect a multitude of users, thus posing complex challenges for regulators and policy makers. Policy makers have to balance protecting users, without stifling innovation and the digital economy.

For some, it is as simple as providing a safe space for users, while for others it could be an issue of national security. The very existence of the internet and its growth is predicated on the premise that it is a safe and trusted space. This is also the bedrock of a growing digital economy and for India's proposed Digital India Act (DIA), a key requirement to achieve a trillion-dollar digital economy by 2026.

While India's laws have recognised user harm in 2021, the DIA offers scope for a more nuanced and effective mechanism to address it. The Information Technology (IT) Act, 2000 does provide us a definition of "user"[1] which is more precise in terms of information technology than the one provided by UK legislations[2], there are several key concepts that are still missing from the current regulatory landscape in India. The IT Rules 2021 imply "user harm"[3] to mean any effect which is detrimental to a user or a child. This definition is very broad and fails to recognise the degrees of harm that need proportionate protections for users.

Most jurisdictions have special provisions for dealing with harms affecting children and minors. However, there is no definitional clarity in Indian law of the age groups that might be more susceptible to certain kinds of online harm. The definition of a "child" in current Indian legislation is a person under 18 years of age. For instance, the UK legislation aims to protect minors from being exposed to harmful content by restricting minors from using social media[4], but the age limits have not been defined. This will not only help platforms to define their users better, while also creating specific protections commensurate with the kind of harms minors could face.

Types of harmful content

Some jurisdictions have provided for a certain kind of classification for what it considers

[1] Sec 2 (x), Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021
[2] Sec 181, Online Safety Bill, UK
[3] Sec 3 (1) (b) Explanation, Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.
[4] Department for Science, Innovation and Technology and Department for Digital, Culture, Media & Sport, 2022. Guidance to Online Safety Bill.

harmful content. These classifications may be based on the size of the platforms, the levels of harm caused by different types of platforms, and so on.

A lot of the jurisdictions require platforms to take steps in relation to illegal content, regarding radicalisation or child sexual abuse material (CSAM). Some jurisdictions go beyond this and aim to regulate content that is "lawful but harmful" such as disinformation (EU, Singapore and the UK) or the promotion of eating disorders (Singapore, Ireland and the UK). Due to concerns about restricting free speech, obligations in respect of "legal but harmful" content for adults have been removed from UK's Online Safety Bill[5]. Even so, the UK and Irish proposals and the Singaporean regime seek to cover the broadest category of harms.

What falls within the purview of illegal content and legal but harmful content varies significantly from jurisdiction to jurisdiction. This is largely decided on the basis of local cultural, social and political considerations. Therefore, an emerging economy such as India has to carefully curate its list of harmful content particular to its aspirations and socio-cultural considerations.

The UK's Online Safety Bill[6], requires platforms to remove content relating to: CSAM, controlling or coercive behavior, cyber bullying, extreme sexual violence, extreme violence against animals or people, fraud, hate crime and speech, inciting violence, illegal immigration and people smuggling, promoting or facilitating suicide, promoting self-harm, revenge porn, selling illegal drugs or weapons, sexual exploitation, and terrorism. This Bill goes a long way in outlining different categories of content that are harmful to children and adults. It provides definitions for:

- illegal content
- primary and priority content harmful to children and adults
- pornographic content, among others[7]

Although this classification might be useful in understanding varying levels of harm associated with different types of content, it might also be difficult to implement. This is so because the categorisation is complex and arbitrary. Instead of following this approach, a better method would be to categorise content into two or three categories based on the grievousness of harm caused, such as illegal content, legal but harmful content, and so on. In Singapore, for instance, the Code of Practice for Online Safety and the Content Code for Social Media Services implements safety standards for six types of content: sexual content, violent content, self-harm content, cyber-bullying content, content that endangers public health and content that facilitates vice and organised crime. The Online Safety Bill in

[5] Hayley Brady, Claire Wiseman, 2023. The Online Safety Bill: A recap of recent changes and their likely impact. Herbery Smith Freehills.
[6] Section 52, Online Safety Bill.
[7] Sections 53 and 54, Online Safety Bill.

Singapore[8] has also defined certain categories of content as "Egregious content"[9]. This includes content that advocates suicide or self-harm, violence or cruelty to human beings, content that exploits the nudity of a child, and content that advocates engaging in conduct that obstructs any public health measure carried out in Singapore.

By providing broad categories of content that are considered harmful and providing a clear definition of "Egregious content", Singapore's legislation makes it easier for platforms to create tools that enable them to comply with these directives better.

Similarly, the proposed DIA can consider defining different categories of illegal and harmful content to better equip platforms to monitor them. India's digital landscape must be cognizant of an emerging category of harms such as addictive tech and content that leads to promotion of suicide or self-harm, among others. Different categories of harms require different sets of responses, and the same regulatory body cannot form mechanisms to address all the harms.

In February 2021, the Indian government introduced new rules under the existing framework of the IT Act, called the "I**ntermediary Guidelines and Digital Media Ethics Code.**" Under these rules, the kind of content that are required to be regulated by Intermediaries includes:

obscene, pornographic or paedophilic content, or content that is invasive of another's privacy.

Gender, **racially or ethnically objectionable content or** content that **promotes money laundering or gambling.**

- Content that is **harmful to child or** i**nfringes any intellectual property rights** is also required to be regulated.

Misinformation/ Disinformation

- **Content that threatens the unity, integrity, defence, security or sovereignty of India**
- Contains software virus or any other computer code, file or program designed to interrupt, destroy or **limit the functionality of any computer resource**;
- Content that is in the nature of an online game that is relating to **gambling or betting or the age** at which an individual is competent to enter into a contract;

These guidelines also place an additional burden on Significant Social Media Intermediaries (SSMIs) to remove content after receiving an order from a competent court or regulatory authority on content that is:

- Damaging to the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, or public order
- Related to rape, sexually explicit material or child sexual abuse material.
- any information which is identical to information that has previously been removed.

[8] Jeremy Tan , Elaina Foo, 2022. Singapore Introduces New Law for Online Safety.
[9] Section 45D, Online Safety (Miscellaneous Amendments) Bill.

This can be interpreted as Illegal content. The onus of addressing illegal content should not just fall on SSMI's alone, but all other kinds of intermediaries. Furthermore, there needs to be an additional classification of legal but harmful content or underage exposure to legal content (such as certain kinds of obscene content).

Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2023 contains a provision for addressing user harm, although the harms that it addresses have been mentioned previously in the IT Act. The most significant change is the extension of the obligations of intermediaries to include gaming intermediaries. Through this amendment, gaming intermediaries have been brought under the ambit of intermediaries and would have the same due diligence obligations that other intermediaries, such as social media intermediaries, would have for addressing user harms. However, this amendment delegates the development of a framework for addressing these user harms on a self-regulatory body. Sec 4A (8) requires every registered self-regulatory body to evolve a framework to include suitable criteria regarding—

- the content of an online game registered with a view to **safeguard users against harm, including self-harm**;
- appropriate measures to be undertaken to **safeguard children;**
- measures to safeguard users against the risk of **gaming addiction and financial loss**, including repeated warning messages at higher frequency beyond a reasonable duration for a gaming session, provision to enable a user to exclude himself upon user- defined limits for time and money spent; and
- measures to safeguard against the **risk of financial frauds**.

As per these rules, the self-regulatory body for gaming will be responsible for safeguarding users against the risk of gaming addiction, financial loss, and fraud[10]. Since user safety is a priority for both legislators and users, the principles of "responsible play" will have to be developed by SRBs. A report by Federation of Indian Fantasy Sports (FIFS)[11] recommends the implementation of guardrails to protect users from psychological and financial harm. Examples of some such measures could be: a mandatory KYC for paying participants to gatekeep minors and prevent duplicate accounts, algorithmic identification of potentially risky behavior, self-exclusion options, time-outs, and voluntary limits on time spent on these apps.

Gaps in Regulatory Framework

There are certain online harms that have been defined clearly in the Indian legislations and some that have a less clear definition. For instance, the term "obscene" is defined under Section 67 of the Information Technology Act, which criminalises the publishing or transmitting of obscene material in electronic form. However, the act does not provide an

[10] Section 4A (8), Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2023.

[11] Fantasy Sports: A catalyst for the sports economy, 2023. Federation of Indian Fantasy Sports and Deloitte.

explicit definition of what constitutes "obscene" content. The interpretation of obscenity is often based on community standards, public morality, and case law precedents.

Courts in India have relied on the three-pronged test established by the Supreme Court in the landmark case of *Ranjit Udeshi v. State of Maharashtra* (1965) to determine obscenity. According to this test, content is considered obscene if it appeals to prurient interests, violates contemporary community standards, and lacks any redeeming artistic, literary, scientific, or social value.

However, it's important to note that the interpretation of obscenity can vary, and what may be considered obscene in one context or community may not be considered so in another. This subjective nature of the definition can sometimes lead to challenges in effectively regulating and addressing online obscenity. While there are provisions in Indian legislations that address certain online harms like obscene content, the precise interpretation and application of these provisions can vary, and clarity in defining certain online harms remains an ongoing challenge.

Clearly defined actions and harms	**Ambiguously defined actions and harms**
• **CSAM and Other Harms to Children:** **Sections 13, 14 and 15 of Protection of Children from Sexual Offenses (POCSO) Act** criminalises the use of a child for sexual gratification. According to Section 13, the use of a child for sexual gratification includes – • representation of the sexual organs of the child; • usage of a child engaged in real or simulated sexual acts (with or without penetration); • indecent or obscene representation of a child. **Section 67B of the IT Act** specifically pertains to children less than 18 years of age and criminalizes any act depicting children in sexually explicit act in electronic form or inducing children to an online relationship for a sexually explicit act. It also criminalizes facilitating the online abuse of children. *The Handbook for Adolescents/Students on Cyber Safety developed by the Indian Ministry*	• **Obscene Content** **Section 292, IPC, Clause 1** lays a list of materials which would be deemed as obscene if it strikes at the lascivious, voyeuristic, salacious or lustful interests of a person and consequently **depraves or corrupts a person in sexual context**. **Section 67 of the IT Act** deals with publishing obscene information in electronic form.

of Home Affairs defines online grooming as "a practice where someone builds an emotional bond with a child through social media or chat window with an objective of gaining their trust for sexual abuse or exploitation" (Ministry of Home Affairs, 2018, p. 9).[3]	
• **Content relating to harassment and intimidation** **Sections 503, IPC** relates to criminal intimidation **Section 504, IPC** criminalizes intentional insult with intent to provoke breach of the peace **Section 509, IPC** criminalizes word, gesture or act intended to insult the modesty of a woman IT Act (**Intermediary Guidelines and Digital Media Ethics Code)** requires Intermediaries to regulate gender, racially or ethnically objectionable content.	• **Content that is harmful to children** **Section 293 of the IPC** deals with a similar subject-matter as Section 292 (obscenity) and punishes any act that constitute sale or distribution of obscene objects to a person under 20 years of age. **67B, IT Act**
• **Financial Harms** Online financial harms refer to fraudulent activities and scams that target individuals or organizations through digital platforms and technologies, with the intention of unlawfully obtaining money or sensitive financial information. These types of harms can have significant financial and personal consequences for the victims. **The following sections of the IT Act address the different kinds of financial harms affecting users:** **Section 43: Penalty and Compensation for damage to computer, computer system, etc** **Section 65: Tampering with Computer Source Documents** **Section 66C: Punishment for identity theft** **Section 66D: Punishment for cheating by impersonation by using computer resource**	• **Content Violating Privacy of a Person:** Section 66E criminalizes any person who knowingly and intentionally captures the image of a private area of a person without his or her consent. ***Justice K.S. Puttaswamy v Union of India:*** A nine judge Bench held that a fundamental right to privacy is guaranteed under the Constitution of India, 1950.

• **Section 66F: Cyber Terrorism** The use of cyber space to cause harm to the general public and disrupt the integrity and sovereignty of the target country	

Therefore, in certain cases, a single offense may fall under the purview of multiple legislations. For example, an act of cyberbullying that involves harassment, intimidation, and threats may attract provisions from both the IT Act and the IPC. This makes it difficult for the law enforcement agencies and the judiciary to choose the appropriate legal provisions based on the nature of the offense and the specific circumstances. Some examples of acts that fall under this category are:

Email Account Hacking If victim's email account is hacked and emails are sent to people in victim's address book, asking for money.

Provisions Applicable: Sections 43, 66, 66A, 66C, 67, 67A and 67B of IT Act.

Credit Card Fraud Unsuspecting victims would use infected computers to make online transactions.

Provisions Applicable: Sections 43, 66, 66C, 66D of IT Act and section 420 of the IPC.

Web Defacement
The homepage of a website is replaced with a hacker's website.

Provisions Applicable: Sections 43 and 66 of IT Act and Sections 66F, 67 and 70 of IT Act

Introducing Viruses, Worms, Backdoors, Rootkits, Trojans, Bugs
All of the above are some sort of malicious programs which are used to destroy or gain access to some electronic information.

Provisions Applicable: Sections 43, 66, 66A of IT Act and Section 426 of Indian Penal Code.

Phishing and Email Scams Phishing involves fraudulently acquiring sensitive information such as passwords, credit card information through masquerading a site as a trusted entity.

Provisions Applicable: Section 66, 66A and 66D of IT Act and Section 420 of IPC

Theft of Confidential Information ***Many business organizations store their confidential information in computer systems. This information is targeted by rivals, criminals and disgruntled employees.***

Provisions Applicable: Sections 43, 66, 66B of IT Act and Section 426 of Indian Penal Code.

Source Code Theft ***A Source code is an important asset of a company and theft of a source code has serious financial implications for any company.***

Provisions applicable: Sections 43, 66, 66B of IT Act and Section 63 of Copyright Act.

Tax Evasion and Money Laundering

Provisions Applicable: Income Tax Act and Prevention of Money Laundering Act. IT Act may apply case-wise.

Online Share Trading Fraud ***It has become mandatory for investors to have their Demat accounts linked with their online banking accounts which are generally accessed unauthorized, thereby leading to share trading frauds.***

Provisions Applicable: Sections 43, 66, 66C, 66D of IT Act and Section 420 of IPC

Measures to be implemented to safeguard against user harm

India's IT Act and subordinate Rules do contain provisions for platforms to remove content on the directives of the Government and empowers users to report harmful content on different platforms. Even so, there is a need to implement better standards for measures that should be taken by intermediaries to address illegal and harmful content. Platforms should be required to produce and publish annual accountability reports on the effectiveness of their safety measures. These could include metrics on how prevalent harmful content is on their platforms, user reports they received and acted on, and the process to address harmful content. These measures would ensure that the principles of user empowerment and risk mitigation will be followed.

In UK's Online Safety Bill, the largest and riskiest Category 1 service providers (such as some social media platforms) will be required to offer adult users tools so they can have greater control over the kinds of content they see and who they engage with online. These tools could include human moderation, blocking content flagged by other internet users or sensitivity and warning screens.

In EU, the Digital Services Act[12] sets out effective means for all actors in the online ecosystem to counter illegal content as well as illegal goods and services. A priority

[12] Paul Haswell and Gordon Tung, 2023. The EU Digital Services Act: Overview and Impact. Seyfarth Legal Update.

channel[13] is created for trusted flaggers (entities which have demonstrated expertise and competence) to report illegal content to which platforms will have to react with priority. When enabled by national laws, Member State authorities will be able to order any platform operating in the EU to remove illegal content[14].

In Singapore, the Online Safety Bill grants power to Singapore's Infocomm Media Development Authority (IMDA) to direct any social media services to disable user access to what the Government deems as 'extremely harmful content', which is determined as content that is related but not limited to suicide and self-harm, sexual harm, public health, public security, and racial or religious disharmony or intolerance, and to disallow specified online accounts from communicating with users in Singapore[15].

Measures specifically aimed at Children

It is clear that there is scope for the DIA to produce a more nuanced legislative framework that provides a higher degree of protection to children, minors and other vulnerable groups from illegal and harmful content, especially as India is demographically a youthful country. It also needs more research to determine who falls under the vulnerable groups category (for instance, divorced/widowed women, orphans, and transgenders). Another important classification that the proposed DIA should address is age segregation among non-adults under 18 years. This would be useful in creating regulations to ensure that minors in a certain category, for instance, under 15, are not allowed on specific platforms such as social media sites.

Measures such as those taken in the UK and Singapore would be effective in mitigating some harms that these groups are more susceptible to. In Singapore, platforms are required to have tools that allow parents and guardians to limit who can connect with their children on social media. It also offers filters that limit what is viewed online, that can be activated by default for users below the age of 18.

Penalties for User Harm

Different jurisdictions have different kinds of penalties for user harm (or contravening any other provisions of their IT legislations). The EU imposes a monetary penalty as well as temporarily limits access to the platform's services. Singapore imposes a monetary penalty, possibility of corporate criminal liability and additionally, requires directors to take down, disable or correct content.

[13] Article 19, Digital Services Act.
[14] Alex Engler, 2021. Platform data access is a lynchpin of the EU's Digital Services Act, Brookings.
[15] Section 45H, Online Safety (Miscellaneous Amendments) Bill.

Jurisdiction	Potential Maximum Fine for the Platform	Possibility of Corporate Criminal Liability	Possibility of liability for individual directors or employees	Other enforcement tools
EU	Up to 6% of global annual turnover, where a provider has been found to breach its obligations For VLOPs, periodic penalty payments up to 5% of the average daily turnover in the preceding financial year per day	No	No	-Requiring commitments from platforms that they will make their services compliant -Temporarily restricting access to the platform's services Periodic penalty payments of up to 5% of the average daily turnover of the platform
United Kingdom	~22 million USD or up to 10% of global annual turnover, whichever is higher, for "failure to comply" with regulatory obligations	No	Yes	-Compel third parties to withdraw key services that make it less commercially viable for the company to operate within the jurisdiction
Singapore	USD 738,000 per non-compliance with a ministerial direction	Yes	Yes	Directions to take down, disable or correct content

The overarching framework for penalties for causing user harm suggests that the loss of safe harbor provision is an extreme measure. This would not be conducive to promoting digital business in India. The Jan Vishwas Bill aims to simplify the compliance requirements for businesses and reducing corporate criminal liability in certain cases with the aim of

enhancing investment opportunities. Monetary penalty seems to be the best way to address user harm, with the option of limiting access to the platform's services only when there is evidence of repeated breaches. The principle of proportionality should be observed while devising penalties for user harm. This will also ensure asymmetrical obligations on intermediaries causing different levels of harm to users. Asymmetrical obligations means that platforms causing higher levels of user harm would have more responsibilities in terms of developing content monitoring and risk assessment tools. They would also have to face higher penalties in cases of contraventions of the regulation's directives, because the magnitude of their effect on users is greater.

2. Principles

1. **Proportional Measures and Penalties**

1.1 Proportionality of the regulations and interventions to the severity of the harm

1.2 Provide safeguards for individual rights and freedoms.

1.3 Define rationale for penalties that do not infringe on fundamental rights.

1.4 Regulators deploy necessary and effective measures for tackling online harms that:

1.4.1 Consider alternative approaches

1.4.2 Minimize unnecessary infringement on fundamental rights

(Explanation: The tools for mitigating online harm must be developed without placing undue burdens on intermediaries. Adequate safeguards and regular reviews should be established to protect against abuses and ensure ongoing accountability)

2. **Risk Assessment and Management**

2.1 Regulatory, including self-regulatory bodies to undertake systematic evaluation of potential risks associated with different types of harm

2.2 Periodic assessments by regulatory, including self-regulatory bodies, enabling the industry to identify:

2.2.1 Specific risks

2.2.2 Likelihood of these risks

2.2.3 Potential impact

2.3 Based on periodic assessments, the regulatory including self-regulatory bodies, must:

2.3.1 Implement appropriate strategies and measures to mitigate and manage the identified risks

2.3.2 Monitor and evaluate to adapt to evolving threats

2.3.3 Ensure efficacy of risk management measures

3. **User Empowerment**

3.1 Equip users with knowledge, tools, and resources to safely navigate digital landscapes

3.1.1 Providing accessible reporting mechanisms for reporting harmful content

3.1.2 Enabling content moderation options

3.1.3 Offering transparent and user-friendly privacy settings

3.2 User-centric design to promote user agency and control over online engagement

3.3 Measures to address misinformation and disinformation

(Explanation: Measures such as community standards or reporting which can provide factual context to claims and assertions on platforms)

4. Transparency and Accountability

4.1 Provide clear communication about the policies, procedures, and enforcement of actions related to harmful content

4.1.1 Platforms should provide users with easy-to-understand and accessible guidelines on acceptable behavior and content standards.

4.1.2 Ensure consistent and fair enforcement of their policies

(Explanation: Regular reporting on content moderation practices – including the number of flagged and removed posts – promotes transparency, accountability and builds public trust. External audits and independent oversight mechanisms can further strengthen accountability)

5. Human Rights and Due Process

5.1 Protect fundamental rights, such as freedom of expression, privacy, and equality

5.2 Adhere to the established legal frameworks and due process while developing measures to address online harm

5.2.1 Ensure users are provided with fair and transparent procedures, such as a Grievance Redressal Mechanism

(Explanation: Safeguards should be in place to prevent arbitrary or disproportionate actions that may infringe upon these rights)

3. User Rights

1. **Right to be forgotten**

(Explanation: The right to be forgotten or the right to erasure is a concept that grants individuals the power to request the removal or deletion of their personal information from online platforms, search engines and other internet mediums. It is closely associated with the right to privacy and data protection in the digital age)

1.1 Balance privacy with public interest, especially when personal information becomes:

1.1.1 Outdated

1.1.2 Inaccurate

1.2.3 No longer serves a legitimate purpose

1.2 Reasonable restrictions should be applied on the grounds of:

1.2.1 Right to freedom of expression and information

1.2.2 Compliance with legal obligations

1.2.3 Performance of tasks in the public interest (such as public health)

1.2.4 Scientific or historical research purposes or statistical purposes

1.2.5 Exercise or defence of legal claims

2. **Right to digital inheritance**

(Explanation: The right to digital inheritance refers to the ability of individuals to transfer or manage their digital assets and online accounts after their death)

2.1 Establish a legal framework for granting fiduciaries (such as executors or trustees) access to a deceased person's digital assets.

2.2 Allow users to specify preferences regarding the disclosure or non-disclosure of digital assets in their estate planning documents.

3. **Right against discrimination**

(Explanation: The right against discrimination includes ensuring equal treatment and non-discrimination in accessing and using digital services. This would include ensuring equal access, opportunities, and treatment for all individuals in the digital realm)

3.1 Prohibition of discriminatory practices based on considerations such as race, colour, gender, religion, sexual orientation, disability, or other factors. This includes

addressing hate speech, online harassment, cyberbullying and other harmful acts that target individuals or groups based on these characteristics.

3.2 The right against discrimination to include procedural safeguards that promote **transparency, accountability and due process.**

4. **Rights against automated/arbitrary decision-making**

(Explanation: The use of automated decision-making systems, such as algorithms and artificial intelligence are associated with risks of potential bias and lack of transparency. Rights against automated decision-making are crucial in ensuring transparency, accountability, and fairness in the use of algorithms and artificial intelligence systems)

4.1 Protect individuals from potential biases, discrimination, and negative consequences that may arise from automated decision-making processes.

4.1.1 Protect user privacy and personal data in the context of automated processing by ensuring fair and lawful processing of personal data, including automated decisions.

5. **Right to privacy**

5.1 Right to privacy was established in the case of ___. To safeguard this fundamental right, there is a need for:

5.1.1 Comprehensive data protection legislation

5.1.2 Encryption technologies

5.1.3 Individual control over digital footprints

Appendix 1.

Section 1: Definitions

Definitions,- In this Act, unless the context otherwise requires,

a) **'Advertisement'** means information designed to promote the message of individuals or entities, irrespective of whether to achieve commercial or non-commercial purposes, and displayed by an online platform on its online interface against remuneration specifically for promoting that information;
b) '**AdTech'** means the software and tools that help agencies and brands target, deliver, and analyze their digital advertising efforts; (US Securities and Exchange Commission)

c) **'Content'** means the electronic record defined in clause(t) of Section 2 of the Act and includes anything communicated by means of an internet service, whether publicly or privately, including written material or messages, oral communications, photographs, videos, visual images, music and data of any description;

d) **'Content moderation'** means the activities undertaken by providers of intermediary services aimed at detecting, identifying and addressing illegal content or information incompatible with their terms and conditions, provided by recipients of the service, including measures taken that affect the availability, visibility and accessibility of that illegal content or that information, such as demotion, disabling of access to, or removal thereof, or the recipients' ability to provide that information, such as the termination or suspension of a recipient's account;

e) **'Cloud service provider'**[16] means a person who makes cloud services available;
For the purposes of this provision:
'Cloud service'[17] means one or more capabilities offered via cloud computing;
'Cloud computing'[18] means the paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.

f) **'Grievance'** includes any complaint, whether regarding any content, any duties of an intermediary or publisher under the Act, or other matters pertaining to the computer resource of an intermediary or publisher, as the case may be;

g) **'Grievance Officer'** means an officer appointed by the intermediary or the publisher, as the case may be, for the purposes of these rules;

h) **'Grievance Appellate Committee'** means a grievance appellate committee constituted under rule 3A;

i) **'Internet intermediaries'**[19] means those persons that bring together or facilitate transactions between third parties on the Internet. They give access to, host, transmit and index content, products and services originated by third parties on the Internet or provide Internet-based services to third parties. Internet intermediaries will fall under three categories[20]:

i) a '**conduit**' means service that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network;

Explanation: For the purposes of this Act, Internet Service Providers will be included under this category.

---

[16] 3.2.15 ISO/IEC 17788:2014(en) Information technology — Cloud computing — Overview and vocabulary. https://www.iso.org/obp/ui/#iso:std:iso-iec:17788:ed-1:v1:en

[17] 3.2.8 ISO/IEC 17788:2014(en) Information technology — Cloud computing — Overview and vocabulary. https://www.iso.org/obp/ui/#iso:std:iso-iec:17788:ed-1:v1:en

[18] 3.2.5 ISO/IEC 17788:2014(en) Information technology — Cloud computing — Overview and vocabulary. https://www.iso.org/obp/ui/#iso:std:iso-iec:17788:ed-1:v1:en. ITU, Cloud computing – Overview and high-level requirements of distributed cloud, 2019. https://www.itu.int/dms_pub/itu-t/oth/06/5B/T065B00001C0043PDFE.pdf

[19] OECD, The Economic and Social Role of Internet Intermediaries, 2010. https://www.oecd.org/digital/ieconomy/44949023.pdf

[20] Article 2(f) EU's Digital Services Act, 2022. https://digitalservicesact.cc/dsa/art2.html

ii) a '**caching**' means a service that consists of the transmission in a communication network of information provided by a recipient of the service, involving the automatic, intermediate and temporary storage of that information, for the sole purpose of making more efficient the information's onward transmission to other recipients upon their request;

iii) a '**hosting**' means a service that consists of the storage of information provided by, and at the request of, a recipient of the service;

Explanation: For the purposes of this Act, Online Platforms will be included under this category.

j) 'Internet service provider'[21] – means a person who provides end-users with a data connection allowing access to the internet and associated services;

k) 'news and current affairs content' includes newly received or noteworthy content, including analysis, especially about recent events primarily of socio-political, economic or cultural nature, made available over the internet or computer networks, and any digital media shall be news and current affairs content where the context, substance, purpose, import and meaning of such information is in the nature of news and current affairs content;

l) 'online gaming intermediary'[22] means any intermediary that enables the users of its computer resource to access one or more online games;

For the purposes of this provision –

'online game'[23] means a game that is offered on the Internet and is accessible by a user

through a computer resource or an intermediary;

Explanation.—In this clause, 'Internet' means the combination of computer facilities and electromagnetic transmission media, and related equipment and software, comprising the interconnected worldwide network of computer networks that transmits information based on a protocol for controlling such transmission.

'online real money game'[24] means an online game where a user pays the service fee charged by the online gaming intermediary and makes a deposit towards the prize pool with the expectation of earning winnings on that deposit;

Explanation.—In this clause, 'winnings' means any prize, in cash or kind, which is distributed or intended to be distributed to a user of an online game based on the

---

[21] OECD, Report on Access Pricing, 2004. https://www.oecd.org/regreform/sectors/18645197.pdf

[22] S. 2(qb) Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2023. https://www.meity.gov.in/writereaddata/files/244980-Gazette%20Notification%20for%20IT%20Amendment%20Rules%2C%202023-%20relating%20to%20online%20gaming%20%26%20false%20information%20about%20Govt.%20business.pdf

[23] S. 2(qa) Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2023. https://www.meity.gov.in/writereaddata/files/244980-Gazette%20Notification%20for%20IT%20Amendment%20Rules%2C%202023-%20relating%20to%20online%20gaming%20%26%20false%20information%20about%20Govt.%20business.pdf

[24] S. 2(qd) Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2023. https://www.meity.gov.in/writereaddata/files/244980-Gazette%20Notification%20for%20IT%20Amendment%20Rules%2C%202023-%20relating%20to%20online%20gaming%20%26%20false%20information%20about%20Govt.%20business.pdf

performance of the user and in accordance with the rules of such online game.

'prize pool' means the total prizes or rewards, in the form of money or money's worth, that is deposited by users participating in an online game, excluding the service fee charged by the online gaming intermediary, which is to be distributed to winners in such online game and that such total prizes or rewards are made known to all participating users in advance of the online game;

'service/platform fee' means the commission or entry amount, in the form of money or money's worth, charged by the online gaming intermediary for provisioning or facilitating or organising the online gaming service to the users, but excludes the deposit or prize pool;

m) 'Online platform'[25] - means a provider of a hosting service which, at the request of a recipient of the service, stores and disseminates to the public information, unless that activity is a minor and purely ancillary feature of another service and, for objective and technical reasons cannot be used without that other service, and the integration of the feature into the other service is not a means to circumvent the applicability of this Regulation;

n) 'Prominently publish' shall mean publishing in a clearly visible manner on the home page of the website or the home screen of the mobile based application, or both, as the case may be, or on a web page or an app screen directly accessible from the home page or home screen;

o) 'Publish', when in relation to intermediaries, means to make content available in electronic form to a potentially unlimited number of third parties, either on demand of the user or by means of a partially or fully automated system(s) that suggest(s) specific information to users in an intermediary's online interface;

Explanation.-- in this clause, "suggests specific information" means suggestions that are a result of a search initiated by a user and includes determining the relative order or prominence of information displayed.

p) 'social media intermediary'[26] means an intermediary 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;

[25] Article 2(h), European Union's Digital Services Act, 2022. https://digitalservicesact.cc/dsa/art2.html

[26] S. 2(w) Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. https://mib.gov.in/sites/default/files/IT%28Intermediary%20Guidelines%20and%20Digital%20Media%20Ethics%20Code%29%20Rules%2C%202021%20English.pdf

q) 'Significant social media intermediary'[27] - means a social media intermediary having number of registered users in India above such threshold[28] as notified by the Central Government;

r) 'search engine'[29] means a service which (a) includes a service or functionality which enables a person to search some websites or databases (as well as a service or functionality which enables a person to search (in principle) all websites or databases); (b) does not include a service which enables a person to search just one website or database;

s) 'Taking action', when in relation to content, means taking down content, restricting users' access to content, or taking other action in relation to content (for example, adding warning labels to content);

t) 'Taking down (content)' means any action that results in content being removed from a user-to-user service or being permanently hidden so users of the service cannot encounter it (and related expressions are to be read accordingly);

u) 'Taking action against a person' means giving a warning to a person, or suspending or banning a person from using a service, or in any way restricting a person's ability to use a service;

v) 'User account' means the account registration of a user with an intermediary or publisher and includes profiles, accounts, pages, handles and other similar presences by means of which a user is able to access the services offered by the intermediary or publisher;

---

[27] S. 2(v) Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. https://mib.gov.in/sites/default/files/IT%28Intermediary%20Guidelines%20and%20Digital%20Media%20Ethics%20Code%29%20Rules%2C%202021%20English.pdf

[28] Ministry Of Electronics And Information Technology Notification New Delhi, the 25th February, 2021 https://www.meity.gov.in/writereaddata/files/Gazette%20Significant%20social%20media%20threshold.pdf

[29] S. 230, UK Online Safety Bill, 2021. https://bills.parliament.uk/publications/52368/documents/3841