

AI Focus

India's Concerns About Deepseek and Possible Regulatory Responses

The launch of open-source large language models (“LLMs”) by [Hangzhou DeepSeek Artificial Intelligence Basic Technology Research Co. Ltd.](#) (“DeepSeek”) has been met with various regulatory responses around the world. News reports [indicate](#) that government departments of several countries are extensively reviewing and/or have already prohibited DeepSeek’s LLMs, including because of [security](#) concerns. While the Commerce Department of the United States [initiated](#) an investigation into DeepSeek’s access to export-controlled chips and later [banned](#) the use of such AI model pursuant to concerns surrounding sensitive government information, Italian regulators [blocked](#) DeepSeek on account of personal data protection issues, potentially leading to European Union-wide [scrutiny](#) related to the General Data Protection Regulation (GDPR). More recently, while a select committee of the US Congress released a [report](#) concluding, among other things, that DeepSeek represents a serious [national security threat](#), the AI model [became available](#) in South Korea only recently after a previously imposed [suspension](#), stemming from perceived [breaches](#) of privacy law, was revoked.

The government of India (“Government”) is currently [monitoring](#) the use of DeepSeek by Indian users, including with respect to the company’s privacy policy and its handling of data flows and storage. If the Government finds it necessary to adopt regulatory measures, it is likely to resort to the framework under the Information Technology Act, 2000 (“IT Act”).

While calls for DeepSeek to be [banned](#) have been made in the Indian parliament, public interest litigation seeking a ban on DeepSeek has also been [filed](#) before the High Court of Delhi. While rejecting a request for an urgent hearing, the court observed that similar data privacy concerns exist with all AI-based models.

The court’s remarks appear to be largely consistent with the Government’s position on AI-based chatbots. In May 2023, the Indian Computer Emergency Response Team (CERT-In) [issued](#) an advisory on AI-based models, flagging data protection and privacy concerns. Recently, the Ministry of Finance [issued](#) a circular prohibiting employees from using OpenAI’s ChatGPT and DeepSeek’s AI-based models for official work and on official devices.

In light of the above, we evaluate the regulatory measures that the Government can potentially deploy to protect Indian citizens and their personal data against privacy and other concerns stemming from LLM-based tools, including AI-based chatbots related to Deepseek, OpenAI’s ChatGPT, and xAI’s Grok.

Regulatory Framework

1. DPDP Act

The Digital Personal Data Protection Act, 2023 (“**DPDP Act**”) was published in the gazette in August 2023 and will come into force on a date to be notified by the Government. For an overview of the DPDP Act, see our note [here](#).

Section 3 of the DPDP Act specifies that its provisions will apply to the processing of personal data outside the territory of India if such processing is in connection with an activity related to the offering of goods or services to data principals within Indian territory. Accordingly, entities operating AI-based chatbots which are accessible to Indian users are likely to be treated as data fiduciaries under the DPDP Act. As data fiduciaries, such entities will be required to ensure that the processing of personal data is undertaken in compliance with provisions of the DPDP Act, including with respect to restrictions on cross-border data transfers.

In general, the DPDP Act obliges data fiduciaries to implement the principle of data minimization. For a discussion on data minimization requirements under the DPDP Act, see our note [here](#). While the DPDP Act requires data fiduciaries to obtain explicit consent from individuals in most instances of personal data processing, such processing can only be done for the specified purpose (pursuant to the principle of ‘purpose limitation’) and must be limited to such personal data as is necessary for such specified purpose (*i.e.*, ‘data minimization’). Accordingly, AI-enabled chatbots will need to evaluate their data collection practices.

The Government has certain powers under the DPDP Act, including the power to restrict the transfer of personal data to a notified country or territory outside India. Recently, the Government issued draft rules under the DPDP Act for public consultation (“**Draft Rules**”). For a summary of the Draft Rules, see our note [here](#). Under the Draft Rules (which are yet to be finalized), the Government may have powers to restrict the transfer or disclosure of personal data to a foreign state or any entity controlled by such foreign state.

Accordingly, once the provisions of the DPDP Act and its rules are notified, the Government can restrict data flows to particular jurisdictions, including with respect to LLMs and AI chatbots. Importantly, AI-enabled platforms could face significant penalties for breaches of prescribed obligations in respect of their data collection, storage and processing practices. Further, like all other data fiduciaries, they will be required to implement appropriate technical and organizational measures to ensure compliance with general obligations under the DPDP Act.

In addition, the DPDP Act has introduced the concept of “significant data fiduciaries”, in respect of which additional obligations apply. Such entities are expected to be notified by the Government based on certain prescribed factors. The Draft Rules specify that such additional obligations include: (a) verifying through due diligence that any algorithmic software deployed for storage, hosting, uploading, transfer or modification of personal data “is not likely to” pose a risk to the rights of data principals; (b) ensuring that certain types of personal data remain in India; and (c) implementing measures to adhere to any specific cross-border transfer restrictions prescribed by the Government.

2. Blocking and Safe Harbor

The IT Act provides for extraterritorial application of its provisions where the offence takes place outside India but includes computer resources located in India. In the past, the Government has resorted to its powers under Section 69A of the IT Act to block access to Chinese websites and applications. Under Section 69A(1), subject to certain procedures and safeguards, and for reasons recorded in writing, the Government may block, or direct an ‘intermediary’ (*see discussion below*) to block, public access to any information that is generated, transmitted, received, stored or hosted in any computer resource under specific circumstances related to national security, public order, and other specified grounds.

In this regard, with respect to safeguards under Section 69A(2) of the IT Act, the [Information Technology \(Procedure and Safeguards for Blocking for Access of Information by Public\) Rules, 2009](#) (“**Blocking Rules**”) deal with the procedure and manner for blocking access.

Intermediaries

An ‘intermediary’ under the IT Act is any entity that:

- receives, stores, or transmits electronic records, messages, data, or other content (together, “**Content**”) on behalf of another entity; or
- provides any service with respect to such Content.

In general, the definition of intermediaries under the IT Act includes telecommunications, internet and web-hosting service providers; search engines; social media platforms; and similar entities.

The principle of ‘safe harbor’ is contained in Section 79 of the IT Act. Being only passive transmitters of Content in respect of, and/or related to, users, intermediaries have been provided immunity from liability under the IT Act with respect to unlawful Content hosted on their platforms. However, safe harbor may be available only as long as such intermediaries satisfy certain conditions. For instance, intermediaries should not select or modify the Content being transmitted. Broadly, safe harbor benefits are contingent upon an intermediary’s due diligence in complying with prescribed obligations in respect of hosting third-party information.

In terms of potential liability for AI-generated Content hosted on an intermediary’s platform, it may be possible for an intermediary to argue that it is immune under the IT Act’s safe harbor principle as long as it can demonstrate compliance with the [Information Technology \(Intermediary Guidelines and Digital Media Ethics Code\) Rules, 2021](#) (the “**Intermediary Guidelines**”). For a discussion on intermediary liability and safe harbor, including with respect to AI-related advisories issued by the Ministry of Electronics and Information Technology (“**MeitY**”) in connection with the Intermediary Guidelines, see our note [here](#).

Importantly, an intermediary loses its immunity if, upon receiving actual knowledge from a court order or a notification from the appropriate government agency that unlawful Content is being hosted on its platform, it fails to expeditiously remove or disable access to such Content. On receipt of a blocking order or take down request under the IT Act, intermediaries are required to prevent

access to the computer resource mentioned in such order or request. For telecom service providers, the obligation to block access to a website or application flows not only from the IT Act, but also from provisions of the telecom license.

Courts in the past have [held](#) that the power of the Government to issue blocking orders under Section 69A of the IT Act is not merely penal and curative, but also preventive. In case the Government anticipates that the operation of an AI-enabled chatbots is a challenge to national security or some such similar concern, it may issue an order blocking access to such chatbot.

Conclusion

The authors submit that the Government has adequate powers under India's existing legal framework under the IT Act to block or restrict access to Content hosted on intermediary platforms, including if it anticipates risks to the security or sovereignty of India. However, the Government's powers under Section 69A of the IT Act to block or moderate Content are not absolute and remain subject to procedural safeguards under the Blocking Rules, as reiterated by the Supreme Court of India pursuant to its landmark [judgement](#) issued in 2015 in the *Shreya Singhal* case.

Nevertheless, with the privacy policy of DeepSeek suggesting that Indian citizens' data may be stored in China-based servers, the Government may take action under the IT Act and its rules to address issues around data transfer and misuse – as it did in the past by banning TikTok, WeChat and several other Chinese apps in 2020.

The Government may also be able to exercise its powers under the DPDP Act and the rules framed thereunder, provisions of which are expected to be notified soon. Such powers include restrictions with respect to cross-border data transfers. Further, the Government could look to implement data localization requirements for certain types of data or require that data from such chatbots is stored or hosted on Indian servers.

Importantly, however, the DPDP Act will not apply to personal data that is made or caused to be made publicly available by data principals themselves. While data from the input prompts provided by users of AI-enabled chatbots may not be made publicly available through direct means, depending on the platform in question and its privacy policy and practices, information contained within such prompts could be used to infer personal data (even if the exact prompt is not publicly displayed) – especially if users feed in sensitive information.

LLM providers should aim to anonymize and de-identify training data to mitigate risks. Among other safeguards, LLM providers could also train their models to not respond to certain prompts. If an LLM is available on an open-source basis (such as Deepseek's models), future deployers can implement the required safeguards themselves.

Concerns related to LLMs and AI-enabled chatbots are not limited to data protection issues alone. In some cases, concerns extend to the responses and output generated by such chatbots, including with respect to politically sensitive issues. Recently, Indian authorities have paid special attention to certain controversial [replies](#) from AI-enabled chatbots such as [Grok](#) and Google's [Gemini](#).

In the past, the MeitY has looked into [concerns](#) about default data collection settings in Chinese mobile phones, including with respect to consent and [cross-border](#) data flows. The widespread [use](#) of Chinese handsets and other devices among Indian users have exacerbated such concerns. While Chinese smartphone companies have faced increased [scrutiny](#) in India, concerns about state surveillance and data leaks [persist](#), along with [security risks](#) and privacy – including in respect of [sensitive personal information](#).

As India's regulatory approach develops further, it would be interesting to see if the Government treats AI-enabled chatbots as intermediaries under the IT Act and/or requires higher diligence standards from such chatbots.

Separately, while India has viewed DeepSeek's [cost-effective](#) approach and multilingual capabilities [favorably](#) and as [inspiration](#) to develop its own [sovereign LLM](#), certain [challenges](#) remain.

The authors further note that the IT Act is likely to be repealed soon and replaced by the Digital India Act (for a discussion on this proposed new law, see our note [here](#)). Given emerging concerns related to data and security, such new laws may incorporate additional checks and balances, safeguards, and obligations.

*This insight has been authored by **Rajat Sethi** (Partner), **Dr. Deborshi Barat** (Counsel) and **Prakriti Anand** (Associate). They can be reached at rsethi@snrlaw.in, d Barat@snrlaw.in and panand@snrlaw.in, respectively, for any questions. This insight is intended only as a general discussion of issues and is not intended for any solicitation of work. It should not be regarded as legal advice and no legal or business decision should be based on its content.*

© 2025 S&R Associates

S&R
ASSOCIATES
ADVOCATES



NEW DELHI

Max House
Tower C, 4th Floor
Okhla Industrial Estate Phase III
New Delhi 110 020
Tel: +91 11 4069 8000

MUMBAI

One World Center
1403 Tower 2 B
841 Senapati Bapat Marg, Lower Parel
Mumbai 400 013
Tel: +91 22 4302 8000