

Because there are no reference points on how much of the content on Facebook will be reported by users under the new law, the workload faced is not calculable.

will have to make use of automated deletion systems, which may infringe on diversity and freedom of opinion, and which may lead users to avoid using such platforms and instead use channels that do not have to adhere to the new law.

If this first attempt by the German authorities to control hate speech fails, the chances are that national lawmakers will embark on new legislative projects once the shortcomings become clear. In light of past experiences it can be assumed that the German legislator will be inclined to tighten the provisions, if the results do not show the required impact. Only seldom does the legislator recognise the ineffectiveness of regulations and lower or reverse legal requirements. It is therefore important that the affected companies do not take the path of least resistance, but rather strive to meet the legal standards in a way that does not impair the user experience.

Social media companies affected by the law should preserve their proactive approach to the issue, not only in order to minimise harmful content, but also in their own best interests. Only if they stay on top of hate speech and fake news can they make sure that they are free to decide which measures are appropriate and apply them in a manner that keeps users satisfied with the experience of their product.

Supreme Court of India rules that privacy is a fundamental right

The Supreme Court of India issued a landmark ruling on 24 August 2017 finding that privacy is a fundamental right guaranteed under Article 21 of the Indian Constitution, in the case *K.S. Puttuswamy v. Union of India*. A nine judge panel of the Supreme Court confirmed that the right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Indian Constitution.

"The ruling is unprecedented from an Indian constitutional law perspective and a harbinger of things to come," said Abhimanyu Baheti and Namrata Bhagwatula of GameChanger Law Advisors. "However, it hasn't explicitly addressed the problem of data protection and informational privacy. In the judgment, Justice Sanjay Kishan Kaul explored the subject of personal data protection. However, his treatise on the 'right to be forgotten' as a means to self regulate data yield appears to be misplaced, given that there is no *sui generis* data protection law in India. The right to privacy does not resolve the practical problems of informational privacy violations if the only recourse to regulating data is in the hands of the very same institutions that are the beneficiaries of such data."

It was confirmed before the Supreme Court that the Government of India has decided to constitute a committee to identify and analyse data protection issues faced in India in order to recommend methods of addressing them, including by way of a new data protection bill. The announcement made by the Ministry of Electronic and Information Technology on 31 July 2016 came in the wake of the deliberations before the Supreme Court.

"The Supreme Court, while elaborating on the advantages and disadvantages of Big Data, also called for a need to regulate the extent to which an individual's information may be stored and used by non-State entities, including for the protection of such information from Governments, which may require that such information be provided to it, by the non-State entity, for national security purposes amongst other reasons," explains Arjun Krishnamoorthy, Associate at J. Sagar Associates. "The Supreme Court also recognised the need to strike a balance between the protection of personal data and the requirements of the State and has recommended that data protection legislation be passed which takes into consideration the need to strike such a balance."

The reasoning advanced in the Supreme Court's ruling will likely impact the forthcoming judgments in the AADHAR case, which is currently pending before a five judge bench of the Supreme Court and which looks at the constitutionality of the AADHAR scheme, which requires all Indian citizens to submit personal data including biometric information in order to be issued with a unique identification number, and the WhatsApp case, which is also before the Supreme Court regarding the viability of WhatsApp's data encryption policy, which is believed to contradict the data sharing arrangement with its parent company Facebook.