Bringing data under the rule of law

Posted at: 20/09/2018

Highlights

- For long, Internet activists considered the Internet as being beyond law, politics and governments.
- J.P. Barlow made the famous **Declaration of Independence of Cyberspace** in 1996.
- But with the Internet and data becoming central to new social and economic institutions, can they still be kept sheltered from the rule of law is matter of question.

Why Data Protection is important?

- It is the law that provides people, especially the weaker sections, various protections and ensures justice.
- In a digital society, as data mirror and help organise all aspects of social, economic and political life, data need to be subject to the rule of law.
- Data are important requirements for various regulations.
- Actors over which the Indian law has no reach should not be able to use our data to harm us through surveillance or informational warfare (including election manipulations).
- Our data should be protected from such foreign entities.

Privacy is a right

- As privacy is a right, it is primarily the state's responsibility to protect our personal data.
- But it can mostly do so only if the data are within its reach.
- There are also great dangers regarding privacy from state agencies themselves.
- Such privacy can only be ensured by invoking and strengthening the protective and corrective powers of the state, including the judiciary and new data protection-related institution(s).
- It will be useful for the new data protection authority proposed by the Srikrishna Committee to actually be a constitutional authority.

Why governments need to access Personal Data?

- Data, and digital intelligence derived from it, are universally acknowledged as the key economic resources in the digital society.
- The European Union, France, the U.K. and some current policy initiatives in India are proposing national data-sharing regimes and data infrastructures.
- This is especially applicable to data taken from public spaces and data that are generated by users on digital platforms, a category called '**community data**' by some current Indian policy texts.
- Such regimes and infrastructures again require the law to have access to potentially

shareable data.
- A lot of privately held digital data are needed for policymaking and governance.
- Some countries are exploring the idea of mandating access to such public interest data.
- The law cannot achieve all these basic objectives if data can easily escape to any part of the world, beyond its reach.
- Countries are therefore developing regulations for storage, processing and cross-border flow of data.
- Global social, cultural, economic and political integration must be promoted, but without sacrificing the effectiveness of nationally organised 'rule of law'. Free flow should be the norm for general information and knowledge, with minimal conditions.
- Treaties should be explored so that data can flow between consenting jurisdictions with guarantees for application of corresponding laws of the country of origin, as the EU has done with its digital single market.
- Employing a liberal regime, the flow of data not considered important for concerned laws should not be hindered.
- Necessary provisions and exceptions need to be shaped for privately owned data which are the kind mostly involved in software and BPO services.
- Entities dealing with data quantities below a certain threshold may be exempted.
- All data flow regulations carry such mitigating provisions, including those proposed in India now.

Data Localisation and Democracy

- Data localisation attempts to bring back the rule of law to our digital and 'datafied' existence.
- All major countries are working on some kind of data localisation proposals.
- Germany, Indonesia, South Korea, Russia and China already have various kinds of data localisation regimes.
- The EU and the U.S. also localise or put very strict conditions on cross-border flow of some kinds of data.
- Global digital corporations live off global data which testifies to their discursive might that when it comes to discussions in developing countries like India, the term '**data localisation**' gets invariably presented as imbued with inherent moral, political and economic evil — a profanity that only state surveillance-minded and economic protectionist people can utter.
- To moral reprobation is added the cost-of-compliance argument.
- While this should be minimised, there is always some cost to maintaining the rule of law.
- There are some accumulated jump-start costs while shifting from a largely lawless regime to the rule of law in the digital space.
- These must be borne if we are to build the foundations of a rule of law-based, fair and just digital society.

What needs to be done?

- The national debate on data localisation needs to integrate a wide range of social, political and economic perspectives.
- Legal and democratic requirements for local data regimes have to be appropriately balanced with the values of global digital integration.
- Interests of a transnational global elite need to be balanced with those whose livelihoods are attached to precarious local economies.

- Fears of state surveillance have to be balanced with the imperatives of a strong enough state that can protect people's interests.
- Data are of many kinds and some of these data are very sensitive, some are needed for effective regulation, some for governance and policymaking, and some for economic development, infrastructure and sharing.
- It is therefore a matter of what kind of data requires what kind of regulatory regime – localisation, global free flow, or various shades of grey in-between, rather than a sterile binary of whether data localisation is good or bad, which is what the debate has been reduced to unfortunately.

The HIndu