A PEOPLES' SUMMIT ON G20

POSITION PAPER ON

DIGITALISATION AND SURVEILLANCE: PRIVACY, DATA RIGHTS AND ACCESSIBILITY

Working Group: Gopal Krishna, Nachiket Udupa, Usha Ramanathan, Apar Gupta, Parmindar Jeet Singh

This position paper is a part of working group papers written for **We20- A Peoples' Summit**, organised in Delhi in the run-up to the G20 Leaders' Summit. The topics for the position papers are agriculture, climate crisis, just energy transition, global economic governance, international trade and development, banking and finance, labour and employment, shrinking democratic spaces (institutions, press freedom, dissent), digitalisation and surveillance: privacy, data rights and accessibility, rising inequality, social protection and welfare, privatisation of public services, gender, health, youth, education, disability rights, debt, inclusive growth, public transport.
Read position papers from other working groups on our website: https://wgonifis.net/g-20/

DIGITALISATION AND SURVEILLANCE: PRIVACY, DATA RIGHTS AND ACCESSIBILITY

Indian context

There are presently three broad approaches to data and information in India.

The first and oldest of the three is the perspective of the right-to-information movement, which holds the view that all the information with the state (with certain exceptions for privacy and national security) should be in the public domain and freely available to anyone.

Subsequently, in response to the widespread imposition of Aadhaar, a nine-judge bench of the Supreme Court of India unanimously recognised privacy as a fundamental right of the citizens of India. Consequently, the government has been attempting to draft a digital data protection law to define the legal contours of the right to privacy.

A third and nascent viewpoint is from the perspective of the economic value of data. While the right to privacy gives people political rights over their data and information, due to the rise of the digital economy, there is also a need to establish a framework for people to be able to meaningfully enjoy the commercial value of their data without exploitation.

Issues

The movement for the right to information is broad-based and has been around for a long time with a well-established point of view. Despite this, in keeping with the way that the government has been ramming through unpopular legislation, the Right to Information (RTI) Act was diluted by amending it to give the government greater powers over the Information Commissions in the first session of Parliament (Monsoon Session of 2019) in the second term of the Modi government. Subsequently, in developments going on at the time that this document is being put together, in 2023 in the last Monsoon Session of the second term of the Modi government, the proposed Digital Personal Data Protection (DPDP) Bill might further dilute the RTI Act.

The DPDP Bill is supposed to operationalise the right to privacy and is also being drafted in a very private manner in both senses of the word. First, most consultations on the drafts of the law are only being done with the private sector. And secondly, the latest and current draft of the bill is not in the public domain. Contrary to established conventions of transparency, the government is being so private with the draft that it has not even shown the draft to the members of Parliamentary Standing Committee on Information and Technology, who were asked to sign on a report about the law!

Further, the versions of the bill in the public domain seem to remove rather than establish boundaries around what the government can do with peoples' personal data by, for example, proposing a Data Protection Board lacking independence or by being silent on surveillance. That a law seeking to provide a legal framework on privacy is completely silent on and ignoring the fact that there are no laws to outline what the state can and cannot do to spy on its citizens is a complete cop out.

In a reflection of the growing trend of the government going after those seeking justice, the proposed law also allows for the Data Protection Board to penalise "frivolous" grievances or complaints, thereby going after the very people it is supposed to protect. And, in classic doublespeak, consent is 'deemed' in several situations - just like Aadhaar is oxymoronically mandatorily voluntary.

Making any digital solution compulsory - be it Aadhaar, app-based attendance in MGNREGA or payments through Aadhaar based or enabled payment systems - in a country where there isn't mobile and internet connectivity everywhere and people are not digitally literate is very impractical. As India tries to leap-frog into the digital age, too many people are falling prey to online scams and losing money due to a lack of adequate digital literacy.

Data protection is not an end in itself. It is the means to protect the people to whom the data pertains. If a data protection law protects only the person's data but not the person itself, then it is not serving its purpose. Globally, most data protection legislation is rightly built on the principle of consent. But the way that consent is usually operationalised in law gives people very little control to protect their data, including the approach that has been adopted so far in India.

Most digital consent frameworks merely allow for a yes or no answer. More sophisticated consent managers allow for more granular sharing of data allowing people to respond to which data they want to share and select which purposes they want to provide consent for. A wider framework which creates space for discussion and allows people to suggest rather than respond to what digital services can do with their data is yet to be properly conceived.

For example, I have little meaningful choice to not use WhatsApp to be in touch with my friends and family as well as for work. Refusing consent to WhatsApp's terms of service practically means staying less in touch with those I love and work with - not a choice most people will make. Similarly, taxi drivers and other gig-workers can't really opt out of terms and conditions of ride-sharing and delivery apps and say no to them since they have EMIs to pay and are financially locked-in. Likewise, current shopping habits make it increasingly hard for retail businesspersons to not be on popular e-commerce websites, often on conditions unfavourable to the sellers. Therefore, meaningful data protection frameworks should allow people to decide how digital services can operate rather than the other way round. This is because, even while consent is obtained in theory, often the real world allows for little choice in practice.

Apart from the surveillance state, data needs protection from those with commercial interests who abuse it against the financial interest of people. Data protection has a privacy component for ensuring political rights of people as well as a commercial component for ascertaining economic rights. By looking at only privacy without safeguarding people's financial interests, legislation will only be taking a

half-hearted approach to data protection. For gig-workers, those selling on online platforms and even people on the internet who receive spookily accurate targeted ads, current data protection regimes will merely assuage symptoms and not address the root cause - the fact that people have very little control on how their data is used beyond a yes or no consent. For genuine people protection, we must create laws that enable participatory governance of the digital services they use so that people can ensure that their data is protected from being used against their interests.

Proposed alternatives and demands

The government must endeavour to provide mobile and internet connectivity at adequate speed to every part of the country. Further, it must run awareness programmes to improve the digital literacy of the population. Digital solutions must not be made mandatory.

The RTI Act must not be amended. When the RTI Act was drafted, Section 8(1)j was included to safeguard privacy of people and has brought a balance and harmony between the rights to information and privacy.

A strong data protection law must be drafted, which meaningfully reigns in the excess of not just corporate big tech but also the state. Therefore, any such proposed legislation must also bring state surveillance within a legal framework.

The Indian government must also begin consultations to create a framework for participatory governance of digital services. Similar to how all those who contribute financial capital (shareholders) have a say in how a financial entity is run; similarly all those who contribute data (capital) to make a digital service viable must have a voice in its functioning.

Conclusion and the role of G20

Just like climate change is a global problem, similarly, the free flow of data and information and an open internet means that there need to be global solutions to digital problems. Merely legislating people-friendly digital laws in India will not fully help since unjust digital services can operate from other jurisdictions and still be accessible and exploitative in India. Rather than choosing to then wall the internet and begin to mandate data localisation, the G20 should play a role in promoting people-friendly digital frameworks all around the world.

To paraphrase Martin Luther King, injustice anywhere online is a threat to justice everywhere online - irrespective of the country.