Data localisation

A matter of rule of law and economic development

Parminder Jeet Singh

Because the law is local

Almost everything in a digital society gets reflected in data. Data contributes digital intelligence which is reorganising us into new social structures and institutions. Data is also the key resource of the digital economy. Any group or nation has a right to manage its data in a manner that best protects and benefits its people. If digital society and economy are to be under the rule of law, obviously data needs to be subject to it. For this, law normally requires physical access to the concerned data. This is the primary rationale for data localisation.

If digital society and economy are to be under the rule of law, obviously data needs to be subject to it. For this, law normally requires physical access to the concerned data.

It was different in the early times when the internet or digital was a side-show to our social organisation and systems. Internet exceptionalism, that allowed the internet and the digital sphere a certain latitude to stay below the radar of law, worked well for that time. It enabled a new model of social interaction and organisation to emerge. We would have been much poorer without it. An inherent globalness is an important element of this new model, which set into motion new cultural, economic and political forces.

The world however remains politically organised along nation states, which apply the rule of law, hopefully in a democratic manner. The new context of a global internet does call for greater international treaties and rules. But any such efforts have been most frustrated by the richest countries who fear that any global rule making would challenge their digital power. For instance, they systematically sabotaged the work of the UN Working Group on Enhanced Cooperation, which had a mandate from the World Summit on the Information Society to explore new global frameworks to govern the internet and digital flows.[1]

With the internet and digital beginning to redefine many social structures and institutions, it is no longer possible to keep the digital space sheltered from the rule of law. As its key element and resource, data too has to be brought under the rule of law. Such efforts should no doubt simultaneously try to accommodate the global nature and possibilities of the internet/ digital. There will be trade-offs in the manner new laws about the digital realm are written and implemented, but enforceable laws there must be. They are needed most to protect the weaker sections, and, in geo-political terms, the developing countries.

Protecting citizens from harm

Demands for localising data to make it subject to the rule of law come from two directions. First is protection of citizens from harm, the main duty of the state. The nature of such harm, and the corresponding remedies, can be individual or collective (a general security threat addressed by a regulation).

Personal data protection is a key concern, since its violation can cause great harm. As with other kinds of personal security, one takes private measures to protect personal data as well as trusts the state to carry out this duty. For the state to ensure protection of people's data, a likely measure is to ordain important data to be kept within locations over which the state's legal realm extends. It is obviously difficult for the state to provide effective protection to data residing in other locations.

It is obviously difficult for the state to provide effective protection to data residing in other locations.

On the other hand, as with one's personhood, one's personal data also needs

1. http://unctad.org/en/Pages/CSTD/WGEC-2016-to-2018.aspx

The only alternative is international treaties whereby rule of origin determines the law to which important data is primarily subject, even as it flows globally.

protection from inappropriate and illegal harm by state agencies. With the state's legal monopoly over use of coercive force, and its all-present might, physical as well as virtual (data related) harms from state agencies are quite likely. However, people address it generally not by escaping one's national jurisdiction but by invoking its protective and corrective powers, and trying to keep improving them internally. Some dissatisfaction with the actions of the authorities of one's country mostly does not mean that one simply withdraws from its jurisdiction and seeks a foreign one! Same goes for data protection and data abuse. For protecting one's data, one would normally have to accept the political jurisdiction of one's citizenship as a package, while striving to keep improving it from within.

Many legitimate and much needed protections provided by the state and the law operate in a collective manner. Regulators and law enforcement often require access to various data, which today is a vital aspect of every social process and structure. It could be needed by the financial regulator, or police investigating a crime or trying to prevent a likely breakout of violence. As everything gets digitalised, this will be true in more and more areas, and more and more often.

In the circumstances, it is unthinkable how the rule of law in digital societies can be maintained without access to data by agencies charged with ensuring the rule of law – though with due procedure and safeguards, which certainly need considerable improvements in the new digital contexts.[2] This imperative of data access requires data localisation in many cases, at least with respect to important data.[3]

The only alternative is international treaties whereby rule of origin determines the law to which important data is primarily subject, even as it flows globally. So that data from a particular country, wherever it may physically be across the globe at a given moment, remains subject primarily to its law. The country of actual physical presence of data will fully cooperate in this matter, not allowing its own laws or any other consideration to interpose in carrying out its treaty obligations. In such circumstances alone can data localisation perhaps be done away with.

Countries of the North are nowhere close to providing developing countries full legal access, and non-interference, with regard to data originating from the latter. In the circumstances, developing countries can only require important data to stay within their own jurisdictions, or allow it to travel within regional or other kinds of groups in which countries mutually agree for such lawful access based on the rule of origin.[4]

A country's economic right to its data

Protection of its citizens from harm is not the only duty of the state. It must also ensure their economic and other forms of well being. Data can not only be used to cause harm (personal data protection), or required to prevent and remedy different kinds of harm (regulatory and law enforcement access), it is also the key resource of the digital economy.

When public spaces and people generate much of the underlying data, should these companies have exclusive ownership over such data capital?

There are currently not enough discussions, much less any laws, on who legitimately owns data, especially the kind that is collected from public spaces. These could be physical spaces, like the roads of a city, or digital ones, like various digital platforms providing publicly available services. These platforms not only collect data that is essential to a particular service, but indiscriminately vacuum up much peripheral user-generated data and unilaterally proprietise and appropriate it. The principle of 'possession is 90% of law' applies, with those collecting and possessing data partaking of its entire economic value.

That the top six companies globally by market value[5] have a business model centred on such data, and its derivatives, tells us how much economic value such data carries. It is not the ownership of manufacturing facilities, nor of intellectual property, but data

2. Data Protection Authorities are being considered in many countries. It will be useful to give them a constitutional status, considering how wide and crucial their task is going to be.
3. The term 'important data' has begun to be invoked in some jurisdictions.
4. As achieved recently in the EU digital single market.
5. https://www.statista.com/statistics/263264/top-companies-in-the-world-by-market-value/

ownership and competence in data processes that puts a company at top of the value chain in every sector. What does Google know about automobiles and Apple about health? They hold virtually no manufacturing or other expertise or intellectual property in these areas, and also not much greater funds, than the traditional automobile and health corporations. But the latter are mortally afraid that Google and Apple can overtake them in these sectors. What is that Google and Apple have which these traditional companies lack? It is data ownership and data-related competences, which can be called as data or digital capital.

When public spaces and people generate much of the underlying data, should these companies have exclusive ownership over such data capital? Or should it be considered like a nation's natural resources, that perhaps get licensed to companies for their business purposes, but within conditions that ensure that the best interests of the concerned nation and its people are served?

Some commentators consider individuals to have economic rights to their data, which they should be able to monetize.[6] Some methods to do so are also suggested, but these are mostly impractical. It is much more practical for groups, including at the level of a nation, to exercise data ownership rights in a collective manner. Importantly, some of the highest value in user generated data is not in its individual form but collective forms. It is the relationships between different data, and the insights emerging from them, which are most valuable. They also underpin artificial intelligence, the new source of all kinds of power.

The very fact that a handful of global data companies make such super-profits indicates that something is wrong with how digital or data value is distributed in the society. The groups or nations from where the basic data comes need to have a much greater share of this digital profit, by the way of license fees, taxes, etc.

Policy-making and governance are fundamentally dependent on statistics and data. Soon it will be impossible to undertake effective governance in most areas without access to large troves of sectoral data which lie with platform companies. Commuting data with Google and Uber that will be required for smart traffic planning is often cited as an example. Similar cases will arise in all sectors. Will public authorities have to pay these companies to get back collective data that the people contributed in the first place? The EU and some developing countries have begun to explore public authorities getting mandated access to such data for the required public purposes.[7]

Will public authorities have to pay companies like Uber and Google to get back collective data that the people contributed in the first place?

Unlike with physical assets, ownership of data is not absolute or exclusive. Companies collecting public or user-generated data can keep profiting from it, as long as at least some of it gets shared for important public purposes. But, as data regimes stabilise on the basis of current norms, whereby whoever collects data can largely do whatever with it, digital companies are not going to share their principal resource for free. It is therefore required to develop clear ownership frameworks around data generated from public spaces and by users on platforms, *inter alia* mandating its sharing for public purposes. No clear frameworks and rules of such a kind exist currently.

An important public purpose is to encourage development of domestic digital industry, as was done for manufacturing in the post-colonial period. For this, domestic industry needs access to general sectoral data, which is largely contributed by a country's public spaces and users collectively, but remains mostly hoarded within global digital corporations.

How can data sharing be mandated if data is freely allowed to travel out to jurisdictions that are unlikely to help in enforcing such economic policies and laws?

EU, France, UK, India, and some other countries are examining how large digital companies can be made to share some sectoral data for enabling the growth of domestic digital industry.[8] Data infrastructures involving shared data are proposed and

6. https://dataflog.com/read/data-ownership-data-usage-consumers-monetize-data/68
7. http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=41205
8. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018DC0232&from=EN, https://www.aiforhumanity.fr/pdfs/MissionVillani_Report_ENG-VF.pdf , https://www.gov.uk/government/publications/artificial-intelligence-sector-deal/ai-sector-deal , https://economictimes.indiatimes.com/news/economy/policy/draft-ecommerce-policy-champions-india-first/articleshow/65206404.cms

The many different kinds of data require different considerations. Just as there cannot be unqualified data localisation, there cannot be unrestricted global flow of data.

being built in all the mentioned countries. The Economist recently suggested 'compulsory licensing' of important data.[9] Such kinds of progressive data policies is the only way for latecomers to undertake digital industrialisation.[10] All developing countries will have to develop some such polices and laws.

How can data sharing be mandated if data is freely allowed to travel out to jurisdictions that are unlikely to help in enforcing such economic policies and laws? A digital ride-hailing company sucks up data about traffic and road conditions, and also user generated data, and then immediately transfers it to a foreign-based sister company which is supposed to provide it data analytics services. Can the country of origin compel getting this data back for sharing for governance purposes or with local industry, on whatever terms that are fair to both sides? And, can it also ensure that the value of collective data is not employed in the foreign country for purposes that are harmful to the people of country of origin, for instance in informational warfare, making smart bombs, etc., or just plain economic exploitation?

Data is so many different things

It is evident that many kinds of data localisation are, and increasingly will even more be, required for ensuring rule of law in a digital society, and for digital industrialisation of developing countries. These are very basic and primary duties of the state to ensure. It is important to move the discussion on data localisation from 'bad nations want to control information even at the risk of economic damage' kind of rhetoric to the really serious issues at hand. While access to data is important for rule of law and digital industrialisation, all efforts should be made to balance these imperatives of data localisation with the aspirations of global integration – cultural, social and economic. Exemptions to data localisation wherever possible – like for privately owned data involved in software and business process services, and operations of multi-national corporations; inter-country agreements for applying legal sovereignty of the country of origin to its data; regional digital single markets with all legal access and economic rights mutually guaranteed; etc., should be explored.

The idea of 'free global flow of data' needs to be divested of some kind of moral superiority over 'data localisation', whose imperative often arise from the high principles of rule of law and economic development.

Data is of so many different kinds; personal, corporate and community data; sensitive, critical and military-value data; infrastructural and sectoral data – in very different areas from transport and energy to health, agriculture, education, and governance; and so on. Each kind has different legal requirements and economic aspects. How a certain kind of data should be treated so that the rule of law and a country's economic interests are best ensured will remain a work-in-progress for quite some time, as a digital society and economy takes shape. It should not be reduced to a sterile binary of 'data localisation or not'. Nor speaking simplistically of 'free global flows of data', as is often done at global trade forums, has any real meaning in an increasingly complex data and digital space. The many different kinds of data require different considerations. Just as there cannot be unqualified data localisation, there cannot be unrestricted global flow of data.

For a start, the idea of 'free global flow of data' needs to be divested of some kind of moral superiority over 'data localisation', which is presented as inherently retrograde. It is the high principles of rule of law and of economic development and justice that provide the rationale for many kinds of data localisation. The alternative to rule of law and progressive digital economy policies is an unchecked rule of the globally powerful, and steeply worsening economic distribution between and within countries.

9. https://www.economist.com/leaders/2018/01/18/how-to-tame-the-tech-titans
10. http://itforchange.net/sites/default/files/1468/Digital-industrialisation-May-2018.pdf