SWP Comment
NO. 10 FEBRUARY 2022

India as an Ambivalent Partner in Global Digital Policy

Potential and Limits of Cooperation in the Digital Economy and Internet Governance

Daniel Voelsen and Christian Wagner

Cooperation in global digital policy is considered one of the most promising fields in the strategic partnership between India and the European Union (EU). However, profound differences are apparent in terms of implementation, for example with regard to data protection, competences of security authorities and the future global digital order. Meanwhile, similar problems are being addressed in the EU's negotiations with the US on digital trade issues. Possible compromises there could also form components of an understanding with India. Shared democratic values are consistently referred to as a justification for efforts to strengthen Europe's cooperation with India. In their Roadmap 2025, India and the EU affirm their interest in promoting an "open, free, stable and secure cyber-space" and fighting cybercrime. But the road to this goal is proving to be rocky.

There is significant potential benefits for both parties if Europe and India become aligned on digital economy issues. For instance, in 2018, only 20 percent of the population in India had access to the Internet, compared to 82 percent in the EU. However, this 20 per cent represented a sizable 270 million people. Moreover, India's digitalisation is expected to continue to advance in the coming years. Therefore, it is attractive for Europe to enter this market of the future. The European market in turn offers great opportunities for Indian companies. For both sides, it is about being able to offer their own services and products as well as creating new opportunities for investment.

Economic Cooperation and Data Protection

Questions of data protection are essential here because processing customer data forms the basis for most digital products and services. However, these can only be traded if the necessary cross-border data transfers are permissible under the relevant data protection law.

This is especially true for applications in the field of artificial intelligence (AI). For instance, some of these data may be company data, such as data from production processes and supply chains. Often, however, the personal data may fall within the scope of the General Data Protection Regu-

Stiftung Wissenschaft und Politik
German Institute for International and Security Affairs

lation (GDPR). Among other things, it stipulates that data subjects must specifically and explicitly consent when their data are transferred from the EU to entities that are not bound by EU law. This can have a deterrent effect on customers and, in any case, results in additional work for all parties involved. To avoid these complications, there is a political mechanism that allows the EU Commission to recognise the adequacy of the data protection requirements of other states. Once this has been done, data transfers to these countries are legally treated in the same way as those within the EU. This means that the data subjects no longer need to give their separate consent to data transfers beyond the borders of the EU. This legal compatibility has already been established for some countries, including Switzerland, Japan and, most recently, the United Kingdom.

However, it is still unclear whether and how an agreement can be reached with the US. In the past, the EU Commission did not issue an adequacy finding to simplify data transfers between the EU and the US. Instead, the EU and the US created contractual mechanisms to deal with the collision of competing norms, namely the Safe Harbor Agreement of 2000 and the Privacy Shield of 2016, which built upon the former.

Like its predecessor, the Privacy Shield 2020 was declared illegal by the European Court of Justice (ECJ). In view of the powers and publicly disclosed practices of the US intelligence services, the ECJ held that EU citizens in the US were not guaranteed that their data would be protected in a way that was roughly equivalent to the level within the EU. Since then, and increasingly since the 2020 presidential election in the US, the two sides have been trying to find a new legal basis for transatlantic data transfer, but so far without success.

Data Protection and Law Enforcement in India

Regarding the EU's relationship with India, the question also arises as to whether Indian data protection law is sufficiently compatible with the requirements of the GDPR. In India, the expansion of online trade and the introduction of electronic administrative procedures such as the Aadhaar card have sparked new discussions about data protection.

The Aadhaar card contains a 12-digit personal identification number, which is intended to provide better and easier access to state transfer payments, especially for the poorer segments of the population. This direct communication is also intended to combat rampant corruption. With the introduction of the card, a political and legal dispute flared up over its functionality and purpose. For instance, there have been numerous reports of counterfeit cards and identity theft. In addition, as part of a test, India's top telecom regulator managed to successfully forge the Aadhaar card.

In 2017, in a decision on the use of the Aadhaar card, the Constitutional Court of India held that the country's constitution grants all citizens a right to privacy. In 2019, the government presented the draft Personal Data Protection Bill, which has not yet passed to date. This means that an essential basis for more intensive cooperation between the EU and India on digital economy issues is missing. Another closely related obstacle is the different powers and control mechanisms of the security authorities.

The latest revelations about the Pegasus spy software have also led to renewed calls in India for greater control of the country's secret services. The software was installed on computers used not only by journalists critical of the government, but also civil servants and military personnel. It thus became clear once again that the country's secret services operate partly without sufficient legal basis and are not subject to parliamentary control. In view of the already increasing authoritarian tendencies in Indian democracy, this scandal has fuelled further concerns about the rampant surveillance of the population with the help of digital technologies. Moreover, some state institutions are already using facial recognition software without any legal basis.

Due to the deficits described above, the Commission or the ECJ are unlikely to come

to the conclusion that European citizens in India are guaranteed a comparable level of data protection as in the EU. The EU has similar problems with the US. For instance, if the EU wants to take its own legal framework seriously, it cannot recognise other legal systems as equivalent in which the European level of data protection is not guaranteed. Beyond the legal details, a political solution is also difficult because of the powers of the intelligence services. The debate thus immediately leads to intricate questions of national security.

India's Ambiguous Stance on Global Internet Governance

Major decisions about the future of digitization are taken at the global level. As such, within the organizational structures of the United Nations, but also in a number of multi-stakeholder formats, negotiations are taking place on the norms that govern the global digital order.

There is clearly a lot at stake here. The structures of the Internet and many of the most important digital services to date were devised in the US. As a result, the global digital order is predominantly shaped by U.S. interpretations of liberal principles. These include enshrining a broad understanding of freedom of expression in the structures of the Internet and encouraging a strong role for private actors in developing and operating digital infrastructures. For many Western countries (including Germany), this liberal approach also implies a clear preference for multi-stakeholder approaches to global Internet governance.

However, the liberal model of the global digital order is now increasingly coming under pressure. On the one hand, the model itself is showing signs of cracks. The global Internet infrastructure, for example, is, in part, technologically outdated, with consequences for both the security and privacy of users. On the other hand, more and more countries are striving to expand control over "their" share of the Internet. The most prominent examples of this are China and Russia, but a number of other states are now following this approach of authoritarian digitization. While most of these states are primarily looking inward, China is also linking this with a claim to reshape the global digital order.

From the point of view of Germany and Europe, it would be attractive to know that India, as a democracy, is on the side of the advocates of a liberal global order. However, in terms of foreign policy, India has consistently promoted national sovereignty and non-interference in internal affairs. Moreover, Indian governments have traditionally emphasized their independence and autonomy in foreign policy matters.

Authoritarian tendencies have increased in India since 2014. Moreover, India has been ranked at the bottom of the Freedom of the Press Index for years and is also the country with the most and longest government-initiated Internet shutdowns.

India's position on the global digital order thus often reflects closer the ideas of authoritarian regimes, as the disputes on global Internet governance forums also show. For many years, the United Nations has been discussing norms regarding the rights and obligations of states in the digital sphere, most intensively in the Group of Governmental Experts (GGE) set up for this purpose. However, the fact that, in 2018, India declared its intention to coordinate closely with Russia on cybersecurity issues, particularly with regard to the GGE process, is a worrying signal.

Voting behaviour in the United Nations General Assembly can serve as a further indicator. Here, too, the results are sobering: on two resolutions on cybercrime, introduced in 2018 (A/RES/73/187) and 2019 (A/RES/74/247), India voted with Russia and thus against the position advocated by Germany and the other EU member states. This is hardly surprisingly given India's foreign policy preference for national sovereignty and non-interference.

This also explains the Indian government's reluctance, or at best ambivalence, toward multi-stakeholder formats of global Internet governance. India is active in some

of these formats, such as the Internet Corporation for Assigned Names and Numbers (ICANN) and the Internet Governance Forum (IGF). At the same time, however, India is advocating a strengthening of the International Telecommunication Union (ITU) as a classic multilateral, intergovernmental counterpart to multi-stakeholder governance.

Difficult Compromises

Cooperation with India on global digital policy would open up two particularly significant opportunities for Europe: first, by facilitating easier access to the Indian market; and second, by engaging India as a partner in the debates on the future of global Internet governance.

In both respects, however, the ambivalence is apparent: on the one hand, there are common interests and values as well as a declared desire for greater cooperation. However, on the other, there are considerable differences. For instance, the lack of a legal framework for data protection and the far-reaching and unclear powers of the Indian intelligence services are hardly compatible with European principles of data protection. India has also repeatedly opposed the efforts of Europe and its allies to establish a liberal digital order in the disputes over global Internet governance.

A simple solution is not in sight: what is needed are sustainable compromises. The Indian Data Protection Act, a new draft which was submitted to India's parliament in December 2021, could provide an opportunity for this. It would be conceivable, for example, for this law or related bills to regulate in a new way the powers of the intelligence services to access personal digital data. Above all, consideration should be given to strengthening the possibilities for judicial review of intelligence activities in this area. Legally and politically, this could form the basis for further discussions on data protection regulations, which, in turn, might eventually pave the way for an adequacy finding by the EU Commission.

The Indian government, however, links the issue of data protection with questions of national security in ways that are hard to reconcile with the EU approach to data protection. Again, the main issue here concerns the largely unchecked powers of India's intelligence services. Therefore, differences over this question are likely to persist.

The situation is similar with regard to Internet governance. Increased cooperation in certain areas is conceivable, but India is unlikely to change its fundamental foreign policy orientation.

The EU must decide for itself what concessions it would agree to and what form these might take. As far as data protection issues are concerned, the EU's current intensive negotiations with the US on similar topics could provide helpful suggestions. Here, too, an agreement will require the EU to make compromises. However, following the ECJ's decision, this will ultimately only be possible if the US, too, is prepared to make certain concessions with regard to the powers of its intelligence services.

Both Brussels and Washington have recognized the urgency of these issues and are under pressure, from the private sector and civil society, to find a solution quickly. The efforts of both sides have thus far been extensive. One initial result is the establishment of the EU-US Trade and Technology Council (TTC). Whether and when the US and the EU will reach agreement on the matter is not yet clear. In any case, however, it seems promising to examine the ideas and approaches put forward in the TTC to see whether they can also be used, in an adapted form, for talks with the Indian government.

Dr Daniel Voelsen is Head of the Global Issues Research Division at SWP.
Dr Christian Wagner is a Senior Fellow in the Asia Research Division at SWP.

SWP
Stiftung Wissenschaft und Politik
German Institute for International and Security Affairs

Ludwigkirchplatz 3—4
10719 Berlin
Telephone +49 30 880 07-0
Fax +49 30 880 07-100
www.swp-berlin.org
swp@swp-berlin.org

ISSN (Print) 1861-1761
ISSN (Online) 2747-5107
doi: 10.18449/2022C10

(Revised English version of SWP-Aktuell 62/2021)