Dawn of a new era of global data protection?

Aishwarya Natarajan, Franziska Rinke, Sebastian Weise

2021-03-02T08:30:10

The recent survey of the United Nations Conference on Trade and Development indicates that 128 out of 194 countries have put data privacy legislations in place. By implication, around 66% of countries in the world have enacted legislations on data protection signifying the importance that states attach to the regulation of information flow in the digital age. The General Data Protection Regulation (GDPR) implemented in May 2018 by the European Union (EU) has marked a new era for data protection across the globe. Although the GDPR serves to harmonize data protection regulations within the EU member states, many countries outside the EU have taken the GDPR as an inspiration. The emergence of the GDPR as a model has decreased differences between data protection frameworks globally, however, the differences have not disappeared entirely. In this context, we seek to explore whether the "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data – No. 108" (Convention 108), the first and only binding international treaty on data protection, will emerge as the basis for a global data protection framework.

Need for a global framework for data protection?

With a view to the fact that data protection laws are implemented on the national level, we could ask: Why is the development of a global framework for the protection of personal data necessary? Due to the massive increase of networked systems and new ways of processing large amounts of cross-border data, personal data in the digital age is exposed to greater risks than ever before. This involves significant risks for the protection of privacy and other human rights. Transnational firms operate across the globe in the areas of finance, health, travel and e-commerce to name a few sectors. Privacy risks include unauthorized use of personal data and a greater exposure to data leaks in a way that was unimaginable in the past. In addition, the big data environment has given rise to unprecedented challenges such as political disinformation campaigns, mass state surveillance and abuse of market dominance by digital platforms. A global framework for the protection of personal data may improve cross-border law enforcement and increases legal certainty for internationally operating companies. A global data protection framework has the potential to: 1) strengthen trustworthy digital innovations; 2) generate economic growth through a free flow of data; and 3) reduce the legal fragmentation of the digital space.

Existing international data protection standards

Since data protection legislation needs to be seen also in the light of the socio-economic background of a country, a one-to-one transfer of the GDPR standards to

other jurisdictions is not a viable option. Additionally, all the ongoing debates about the GDPR in Europe and beyond clearly underline that creating an effective well balanced data protection legislation is a protracted process. This process becomes all the more complicated if the concepts of data protection, data sovereignty and innovation are to be reconciled. In order to achieve greater global acceptance, it seems more reasonable to look for principles and standards with a level of data protection more countries can agree on. This will certainly increase the willingness to implement a global standard even in countries with a rather low level of data protection so far.

Since the 1980s, the first and only binding international treaty on data protection is the Convention 108. Until now, 55 states (including all member states of the Council of Europe (COE)) have ratified/acceded to this treaty. The Convention 108 is not limited to the member states of the COE. It is open to accession by non-member states (currently Argentina, Burkina Faso, Cabo Verde, Mauritius, Mexico, Morocco, Senegal, Tunisia and Uruguay have signed and ratified the Convention 108), provided that they have been formally invited to accede by the Committee of Ministers of the COE. This fact makes it more attractive as a Global Data Framework. Convention 108 protects the individual against abuses which may accompany the collection and processing of personal data and seeks to regulate at the same time the trans-frontier flow of personal data. In 2018, the COE updated the treaty in order to address the challenges for privacy resulting from the use of new information and communication technologies; and to strengthen the convention's follow-up mechanism. The modernisation process also aimed at bringing together the various normative frameworks that have been developed in different regions of the world. The modernised Convention 108, also referred to as Convention 108+ ('C108+'), has been open for signature since 10 October 2018. There are two roads open for the convention to enter into force: First, when all parties to the existing Convention 108 have ratified it; or alternatively on 11 October 2023, provided that 38 parties have ratified the treaty by this date. Although 43 countries have already signed the treaty, the total number of ratifications/accessions stagnates at ten. Given that the GDPR has had a "spillover effect", it is not entirely unlikely for C108+ to enter into force, especially if the EU promotes the diffusion of C108+ in cooperation with like-minded partners.

Next steps

Despite the momentum for a global legal framework to protect personal data, the road to establish C108+ is a challenging one. It is not only multilateralism that is in crisis worldwide. C108+ is also a treaty strongly based on liberal and European values. The GDPR and C108+ are, so to say, cut from the same cloth. The accession to C108+ implies compliance with most aspects of the GDPR. Potential accession countries could be those countries for which the EU has adopted a positive adequacy decision, e.g. Canada, Japan, New Zealand, Argentina and Uruguay (with Uruguay and Argentina already having ratified Convention 108). The EU Commission has the power to determine, whether a country outside the EU offers adequate level of data protection using the adequacy decision mechanism. In addition, the EU should work towards the accession of Brazil, Australia, South

Korea, Chile and India to C108+. These countries already have legal frameworks comparable to the GDPR, which could potentially be compatible with C108+. Moreover, broad support by these countries would strengthen the legitimacy of C108+ as a global framework. While the U.S. could also be a supporter of C108+, the approach of the new U.S. government remains yet uncertain. With these states as potential partners, both the G7 and G20 – with its enormous market power – uniting behind C108+, could pave the way for a global data protection framework. Therefore, Europe should debate data protection issues more intensively with non-European expert communities in the field of data protection. Further support is expected from UN side. Already in 2018, the UN Special Rapporteur on the right to privacy called on UN member States to ratify Convention 108+.

Conclusion

The GDPR and its "spillover-effect" has demonstrated that the EU can be a leading norm entrepreneur to promote a global data protection framework. The GDPR has opened up a window of opportunity for a global data protection framework in the digital age. However, in order for the C108+ to emerge as the universal norm, it is critical to understand and to address the hurdles faced by non-EU members, especially in the developing world, in adopting such a measure. Countries across Asia, Africa and Latin America have experienced a rapid growth of successful technology start-up ventures, which have provided significant socio-economic benefits to these societies. Therefore, a new global standard that regulates data must necessarily ensure that there are no adverse economic impacts for these countries. The EU should consider ways to mitigate such adverse impacts as well as increase economic incentives to signatories of the C108+. One such obvious interest is of course the access to EUs digital single market itself.

The second issue that requires more careful consideration is the differing state capacity across the globe to effectively implement a global data protection standard. While signing a treaty and legislating a new law is a relatively achievable target, we have to explore whether a strong regulatory environment with enforcement mechanisms is possible for states with limited governance and financial resources. The EU should consider ways to provide regulatory and technological assistance to developing countries to tide over this hurdle.

Further, a user consent-based legislation like the GDPR assumes a high level of digital literacy. The digital divide in the developing world is wide and hence this consent will be meaningless if there are no concentrated efforts to bridge the digital divide. The EU could consider ways in which it can support the efforts of non-EU member states in bridging the digital divide. In fact, the European Commission's "Digital4Development" strategy lists promotion of digital literacy skills as one of its core priority areas. Under this umbrella, the EU offers support to partner countries to draft digital skills and literacy strategies and to adapt curricula to integrate digital skills and literacy into their educational system including training of teachers. As indicated in the Digital4Development strategy, EU can also assist partner countries in other areas such as improving digital infrastructure, undertaking regulatory reforms, fostering digital entrepreneurship and promoting the use of digital technologies. The EU is already engaged in several projects with African states

on these topics. The EU's active assistance in these areas itself could serve as an incentive to join the C108+. In the light of these challenges, one final conclusion needs to be stressed: A Global Data Protection Framework is important but will require a strong and broad-based political will.
