National Law School of India Review

Volume 33 | Issue 1 Article 4

2021

The Path To Recognition of Data Protection in India: The Role of the GDPR and International Standards

Christopher Kuner

NLSIR

THE PATH TO RECOGNITION OF DATA PROTECTION IN INDIA: THE ROLE OF THE GDPR AND INTERNATIONAL STANDARDS

—Christopher Kuner*

Abstract By providing rules of the road for data processing, data protection legislation has become a key enabler of the information society. The European Union's General Data Protection Regulation (GDPR) has been highly influential around the world, and the recent *Schrems II* judgment of the Court of Justice of the EU, which strengthened restrictions on international data transfers under EU law, has important implications for India as it prepares to adopt data protection legislation. While the *Puttaswamy* judgment that recognised privacy as a fundamental right represents a great stride forward for privacy protection in India, legislation is necessary to establish the right to data protection in the Indian legal system. The proposed Personal Data Protection Bill does not provide a sufficiently high standard of data protection, particularly in light of surveillance initiatives and legal mandates to collect data under Indian law. India should view the strengthening of its legal framework for data protection not just as a way to receive an EU adequacy decision, but also as having broad societal benefits. In adopting data protection legislation India should align itself both with the GDPR and also more broadly with data protection standards of important international bodies, such as those of the Council of Europe and the OECD.

* Professor of Law, Vrije Universiteit Brussel (VUB) and Co-Director, Brussels Privacy Hub, Brussels, Belgium. The author is grateful to the editors and the anonymous reviewers for their helpful comments.

I. INTRODUCTION

International data flows have increased dramatically in complexity and volume in recent years.[1] Data transfers have become ubiquitous, while often remaining hidden from the individuals who use information technology, and personal data routinely flow across national borders. These developments have led to the creation of new technologies, products, and services, but have also created risks for the misuse of personal data.

The changing nature of global data flows has been accompanied by a rise in laws designed to strengthen the rights of individuals in the processing of their personal data. This is referred to as data protection, and can be viewed as a set of rules designed to grant rights to individuals in the processing of data that may identify them, and to provide 'rules of the road' for data processing.[2] Most countries in the world have enacted data protection legislation,[3] and the most influential set of data protection laws have been those of the European Union ('EU'), in particular the former EU Data Protection Directive 95/46/EU[4] (the Directive, which is no longer in force), and its successor, the EU General Data Protection Regulation ('the GDPR').[5] EU data protection law can also have an impact on countries outside the borders of the EU (so-called 'third countries' in EU parlance),[6] and the EU has attempted to position the GDPR as the global standard for data protection.[7]

---

1 *See*, Lee Bygrave, *Data Privacy Law: An International Perspective* (OUP 2014, Kindle edition) 1203; Christopher Kuner, *Transborder Data Flows and Data Privacy Law* (OUP 2013) 1-7.

2 *See*, regarding the definition of data protection, Bygrave (n 1) 1123-1198; Peter Hustinx, 'EU Data Protection Law: The Review of Directive 95/46/EC and the General Data Protection Regulation' in Marise Cremona (ed), *New Technologies and EU Law* (OUP 2017) 125-131.

3 *See*, Graham Greenleaf and Bertil Cottier, '2020 Ends a Decade of 62 New Data Privacy Laws' (2020) 163 Privacy Laws & Business International Report 24 <https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3572611_code57970.pdf?abstractid=3572611&mirid=1> accessed 1 April 2021, stating that as of 2020 there were 142 countries with data privacy laws.

4 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31.

5 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.

6 *See*, Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (OUP 2020, Kindle edition) 132-136; Christopher Kuner, 'The Internet and the Global Reach of EU Law' in Marise Cremona and Joanne Scott (eds), *EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law* (OUP 2019) 112-145; Paul M Schwartz, 'Global Data Privacy: The EU Way' (2019) 94 New York University Law Review 771; Graham Greenleaf, 'The Influence of European Data Privacy Standards Outside Europe: Implications for the Globalisation of Convention 108' (2012) International Data Privacy Law 68.

7 *See*, the following statement by two European commissioners: Věra Jourová and Didier Reynders, 'Joint statement ahead of the second year anniversary of the General Data Protection Regulation', (European Commission, 20 May 2020), <https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_20_913> accessed 3 May 2021, stating with regard to

One of the most significant features of EU data protection law is the fact that it restricts the transfer of personal data to third countries (including to India) unless certain conditions are fulfilled. The European Commission ('the Commission'), which is the executive arm of the EU, may issue a formal adequacy decision recognising that a third country provides an adequate level of data protection based on EU standards, which then allows personal data to flow freely to it.[8] Failing an adequacy decision, data transfers may also be legalised by the use of 'appropriate safeguards', which most frequently entails the use of standard contractual clauses ('SCCs').[9] These are standardised form contracts for data transfers that are formally adopted by the Commission and are entered into between the party(ies) in the EU that transfer the data and those outside the EU that receive them, and obligate the parties to provide protections for the data during the transfer and when they are received and processed in the third country.[10]

Data protection legislation is essential to protect the rights of citizens and to provide trust for online services. In addition, it helps facilitate initiatives that are essential for the public good, since many individuals may be unwilling to participate in the wide-ranging data gathering that such initiatives entail without there being a legal framework in place to protect their data (e.g., with regard to data-gathering for the purpose of combatting the COVID pandemic[11]). Data protection also has a substantial economic importance, particularly for a country like India with a strong digital services industry that is dependent on being able to receive data freely from other regions.[12] The EU

---

the GDPR: "Within two years, these rules have not only shaped the way we deal with our personal data in Europe, but has also become a reference point at global level on privacy". Regarding the global reach of EU data protection law in general, *see,* Kuner (n 6).

8 GDPR, art 45.

9 GDPR, art 46(2)(c).

10 The SCCs are available at <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en> accessed 7 May 2021. The SCCs at issue in *Schrems II* were those that had been approved by Commission Decision 2010/87 and later amended by Commission Decision 2016/2297. *See*, Commission Decision (EC) 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive (EC) 95/46/EC of the European Parliament and of the Council [2010] OJ L 39/5; and Commission Implementing Decision (EU) 2016/2297 of 16 December 2016 amending Decisions 2001/497/EC and 2010/87/EU on standard contractual clauses for the transfer of personal data to third countries and to processors established in such countries, under Directive 95/46/EC of the European Parliament and of the Council [2016] OJ L344/100.

11 *See*, eg, European Data Protection Board, 'Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak' (21 April 2020) 3, stating "The EDPB firmly believes that, when processing of personal data is necessary for managing the COVID-19 pandemic, data protection is indispensable to build trust, create the conditions for social acceptability of any solution, and thereby guarantee the effectiveness of these measures".

12 *See*, eg, CUTS International, *Data Localisation: India's Double-Edged Sword?* (2020) 11-12.

is one of India's major trading partners,[13] and the Indian government and the EU have recently "reaffirmed their commitment to work towards balanced, ambitious and mutually-beneficial trade and investment agreements, opening markets and creating a level playing field on both sides".[14]

However, privacy and data protection are not just economic issues, but are also important for the protection of fundamental rights in general and the functioning of democracy.[15] This has been stated powerfully by the Supreme Court of India:

> It is privacy as an intrinsic and core feature of life and personal liberty which enables an individual to stand up against a programme of forced sterilization. Then again, it is privacy which is a powerful guarantee if the State were to introduce compulsory drug trials of non-consenting men or women. The sanctity of marriage, the liberty of procreation, the choice of a family life and the dignity of being are matters which concern every individual irrespective of social strata or economic well being. The pursuit of happiness is founded upon autonomy and dignity. Both are essential attributes of privacy which makes no distinction between the birth marks of individuals.[16]

In its 2017 *Puttaswamy*[17] decision, the Supreme Court of India recognised a constitutional right to privacy against the State. However, data protection is a subset of the right to privacy but not identical to it,[18] so that recognising the right to privacy is not the same as having a legal framework for data protection. Data protection law applies to data processing even when it may not involve the privacy of the individual, and is thus often broader than privacy since it covers a wider scope of data.[19] India currently lacks omnibus data protection legislation (i.e., legislation recognising data protection broadly over

---

[13] According to the European Commission, "The EU is India's largest trading partner, accounting for €80 billion worth of trade in goods in 2019 or 11.1% of total Indian trade, on par with the USA and ahead of China (10.7%)". European Commission, 'Countries and regions: India' <https://ec.europa.eu/trade/policy/countries-and-regions/countries/india/> accessed 9 May 2021.

[14] *See,* Ministry of External Affairs, Government of India, 'Joint Statement of the 15th India-EU Summit' (Ministry of External Affairs, July 15 2020) <https://www.mea.gov.in/bilateral-documents.htm?dtl/32827/Joint_Statement_of_the_15th_IndiaEU_Summit_July_15_2020> accessed 9 May 2021. In February 2021 the first meeting of a new EU-India High-Level Dialogue on Trade and Investment was held. European Commission, 'EU and India launched the High-Level Dialogue on Trade and Investment' (European Commission, 6 February 2021) <https://trade.ec.europa.eu/doclib/press/index.cfm?id=2242> accessed 9 May 2021.

[15] *See,* Alan Westin, *Privacy and Freedom* (Atheneum 1970) 23-51.

[16] *KS Puttaswamy v Union of India* (2017) 10 SCC 1 [157].

[17] ibid.

[18] *See,* Orla Lynskey, *The Foundations of EU Data Protection Law* (OUP 2015) 89-106.

[19] *See,* Hustinx (n 2) 127.

a wide range of data processing situations), though the government has introduced a draft Personal Data Protection Bill[20] which was still being debated when this article was finalised.

This article will examine the implications for India posed by EU rules on data protection and international data transfers, particularly in light of the GDPR and the judgment of the Court of Justice of the European Union ('CJEU' or 'the Court', the highest court in the EU legal system) of 16 July 2020 known as *'Schrems II'*.[21] In this judgment, the Court made important pronouncements dealing with the transfer of personal data that have significant implications for India's quest for an adequacy decision from the EU. In addition, following the judgment, the European Commission published a decision with a new set of SCCs,[22] and the European Data Protection Board ('EDPB'), which is the group of European data protection authorities ('DPAs')[23] charged with ensuring consistent application of the GDPR,[24] published two recommendations that specify the conditions under which the SCCs are to be used.[25] Since the SCCs frequently serve as a legal basis for data transfers from the EU to India, the *Schrems II* judgment and the regulatory developments it has engendered have important implications for the private sector in India as well. They also raise questions about the methodology used by the EU to decide on the level of data protection in third countries.

Finally, conclusions will be drawn about the role that EU adequacy has for India as it confronts its choices in adopting data protection legislation. It will focus in particular on the importance of India adopting a high standard of data protection, complying with international legal standards, and becoming more involved in international discussions, as a way to place itself in the international data protection mainstream.

---

[20] Personal Data Protection Bill, 2019, Bill No 373 of 2019, <https://www.prsindia.org/sites/default/files/bill_files/Personal%20Data%20Protection%20Bill%2C%202019.pdf>.

[21] *Data Protection Commr v Facebook Ireland Ltd and Maximilian Schrems*, Case C-311/18 [2020] ECLI:EU:C:2020:559.

[22] European Commission, 'Commission Implementing Decision (EU) …/… of 4.6.2021 on standard contractual clauses for the transfer of personal data to third countries pursuance to Regulation (EU) 2016/679 of the European Parliament and of the Council', C(2021) 3972 final, 4 June 2021.

[23] DPAs are independent public authorities that exist in all EU Member States and at EU level and are charged with enforcing the law and protecting the rights of individuals. They are supposed to work in complete independence, and are thus not part of any government department or ministry.

[24] *See*, GDPR, art 70(1).

[25] EDPB, 'Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data' Version 2.0 (18 June 2021); 'Recommendations 02/2020 on the European Essential Guarantees for surveillance measures' (10 November 2020).

II. THE *SCHREMS II* JUDGMENT AND ITS IMPLICATIONS

A. The judgment and its background

The Austrian law student and privacy activist, Max Schrems, complained in 2013 to the Irish Data Protection Commissioner ('DPC') about transfers by Facebook of his personal data to the US. After his complaint was rejected, he then brought an action before the Irish High Court, which referred a number of questions to the CJEU concerning the validity of the EU-US Safe Harbour arrangement that provided the legal basis for Facebook's data transfers and which the European Commission had found in a formal decision to provide an adequate level of data protection for data transfers to the US.[26] The Safe Harbour was a self-regulatory mechanism that required US commercial entities that joined it to provide a set of agreed safeguards to personal data transferred to them from the EU, backed up by the enforcement powers of the US Federal Trade Commission ('FTC'). In a judgment of 6 October 2015 (referred to here as '*Schrems I*'), the CJEU invalidated the Safe Harbour decision, and held that an adequate level of data protection required that third country law be 'essentially equivalent' but not necessarily identical to EU law.[27] The High Court then annulled the decision rejecting the complaint and referred the case back to the DPC.

The focus of Schrems' complaint before the DPC then shifted to Facebook's use of the SCCs for data transfers to the US. He complained that the SCCs could not provide a valid legal basis for such transfers, in part because Facebook was obliged to make the personal data of its users available to US government authorities in the context of their surveillance programs. After investigating Schrems' allegations and finding that it could not adjudicate on them until the CJEU examined the validity of the SCCs, the DPC then brought proceedings before the High Court. The complaint also raised questions about the level of protection provided by the EU-US Privacy Shield, which was a self-regulatory mechanism requiring member companies in the US (of which Facebook was one) to provide defined protections to personal data transferred from the EU, much like the Safe Harbour arrangement described above. The Privacy Shield had also been formally recognised by the European Commission as providing an adequate level of data protection.[28]

---

[26] European Commission Decision 2000/520 of 26 July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbor privacy principles and related frequently asked questions issued by the US Department of Commerce [2000] OJ L 215/7 (annulled).

[27] Case C-362/14, *Maximillian Schrems v Data Protection Commissioner*, judgment of 6 October 2015 (Grand Chamber) (ECLI:EU:C:2015:650) [73].

[28] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection

On May 9, 2018, the Irish High Court stayed the proceedings and referred a number of questions to the CJEU. In his Opinion in the case delivered on December 19, 2019, Advocate General Saugmandsgaard of the CJEU[29] examined the questions referred to the Court under both the Directive and the GDPR, which in the meantime had become fully applicable.[30] He upheld the validity of the SCCs and found that there was no need for the Court to examine the validity of the Privacy Shield, though he did have questions about the level or protection it provided.

In its judgment in *Schrems II*, the Court of Justice summarised the questions referred to it by the Irish High Court in five broad categories, as follows: (1) whether the GDPR applies to data transfers between economic operators in situations where the data are likely to be processed in a third country for public security and law enforcement purposes;[31] (2) what level of protection applies under the SCCs;[32] (3) whether the DPAs are required to suspend or prohibit data transfers under the SCCs if in their view the clauses are not complied with or the level of protection cannot be ensured;[33] (4) whether the SCCs are valid under the EU Charter of Fundamental Rights[34] ('the Charter');[35] and (5) whether the Privacy Shield ensures an adequate level of protection under the GDPR.[36]

The Court rejected various objections that the GDPR did not apply to the case,[37] and also found that the fact that national security is placed within the sole responsibility of the Member States under EU law could not affect the applicability of the GDPR in this case.[38] It held that the standard of essential equivalence with EU law which it had found to apply to adequacy decisions in *Schrems I* also applies to data transfers under the SCCs,[39] and confirmed that the standards for determining the level of protection must be based on EU law, particularly the Charter.[40] Within these parameters, the Court upheld the use *per se* of SCCs as a data transfer mechanism.[41] However, it also found

provided by the EU-U.S. Privacy Shield [2016] OJ L 207/1.

29 The Advocates General are Members of the Court of Justice who present opinions to the Court in cases assigned to them. Their opinions are not binding, but are highly influential and are often followed by the Court.

30 Case C-311/18, *Data Protection Commr v Facebook Ireland Limited and Maximilian Schrems* (ECLI:EU:C:2019:1145), Opinion of Advocate General Saugmandsgaard. The GDPR because fully applicable on 25 May 2018.

31 *Schrems II* (n 21) [80].

32 ibid [90].

33 *Schrems II* (n 21) [106].

34 Charter of Fundamental Rights of the European Union [2010] OJ C83/2.

35 *Schrems II* (n 21) [122].

36 ibid [160].

37 *Schrems II* (n 21) [82]-[85].

38 *Schrems II* (n 21) [81].

39 *Schrems II* (n 21) [96].

40 *Schrems II* (n 21) [99].

41 *Schrems II* (n 21) [136].

that since SCCs do not bind public authorities (such as law enforcement or security authorities) in third countries, they cannot restrain such authorities from accessing data transferred under them. Therefore, the Court held that the contracting parties should make use of 'additional safeguards' to protect the data in addition to those provided under the SCCs,[42] though it did not provide details as to what such additional safeguards should be; they have since been specified in the guidance from the EDPB.[43]

The Court also affirmed the principle of accountability with regard to international data transfers. Accountability is an important principle of the GDPR that requires data controllers to be able to demonstrate compliance with the main principles that they must abide by when processing personal data.[44] Thus, the Court stated that data controllers transferring data under the SCCs must "verify whether the law of the third country of destination ensures adequate protection under EU law",[45] and that they "are required to verify, prior to any transfer, whether the level of protection required by EU law is respected in the third country concerned".[46] In addition, the Court confirmed the duty of the DPAs to suspend or prohibit data transfers if the SCCs cannot be complied with or if protection of the data cannot be otherwise ensured.[47]

In the final part of the judgment, the Court invalidated the Commission Decision that was the legal basis of the Privacy Shield. The Court's invalidation of the Privacy Shield was based on several factors, namely: (1) the primacy of US law enforcement requirements over those of the Privacy Shield;[48] (2) a lack of necessary limitations and safeguards on the power of the authorities under US law, particularly in light of proportionality requirements;[49] (3) the lack of an effective remedy in the US for complaints by EU data subjects;[50] and (4) deficiencies in the Privacy Shield Ombudsman mechanism.[51]

B. Subsequent developments

Following the *Schrems II* judgment, the Commission and the EDPB issued important documents clarifying some of the major points made in it. The

---

42 *Schrems II* (n 21) [134].
43 *See*, EDPB Recommendations 01/2020 and Recommendations 02/2020 (n 25).
44 *See*, GDPR, arts 5(2) and 24.
45 *Schrems II* (n 21) [134].
46 *Schrems II* (n 21) [142].
47 *Schrems II* (n 21) [113].
48 *Schrems II* (n 21) [164].
49 *Schrems II* (n 21) [168]-[185].
50 *Schrems II* (n 21) [191]-[192].
51 *Schrems II* (n 21) [193]-[197].

Commission produced a decision[52] containing a new set of SCCs,[53] while the EDPB published recommendations on supplementary measures to use together with the SCCs[54] and recommendations on 'European essential guarantees for surveillance measures'.[55] These documents result in the judgment's holdings being implemented in the practice of international data transfers, and thus have substantial impact on transfers in the private sector as well.

C. A high standard of protection

In its two *Schrems* judgments, the CJEU set a high bar with regard to the level of protection for international data transfers. In *Schrems I*, the Court made it clear that while third country law need not be identical with EU law, it must be evaluated in light of the Charter,[56] meaning that ultimately the level of protection will be judged against the high standards of EU fundamental rights law.

It is important to mention that the horizontal scope of fundamental rights differs between legal systems.[57] EU fundamental rights law is not *per se* limited to violations by the State, but may, depending on the particular right, its implementation, and the circumstances involved, also be asserted horizontally, i.e., against private parties; this includes the right to data protection.[58] The GDPR also applies horizontally to both the public and private sectors, with some exceptions.[59] This differs from the situation in India, where fundamental rights provide a remedy against a valued interest by the State,[60] but not necessarily against private actors.

The CJEU expounded on what constitutes essential equivalence with EU data protection law in *Schrems I*, and set out the following requirements for this standard to be met:

1. There must be a high level of fundamental rights protection, which must be evaluated strictly.

---

52 European Commission, 'Commission Implementing Decision (EU) …/… of 4.6.2021 on standard contractual clauses' (n 22).

53 European Commission, 'Annex to the Commission Implementing Decision on standard contractual clauses for the transfer of personal data to third countries pursuance to Regulation (EU) 2016/679 of the European Parliament and of the Council', C(2021) 3972 final, 4 June 2021.

54 EDPB, 'Recommendations 01/2020' (n 25).

55 EDPB, 'Recommendations 02/2020' (n 25).

56 *Schrems I* (n 27) [73]; *Schrems II* (n 21) [99].

57 *See*, Jenny S Martinez, 'Horizontal Structuring' in Michel Rosenfeld and Andras Sajó (eds), *The Oxford Handbook of Comparative Constitutional Law* (OUP 2012, Kindle edition) 4511-4590.

58 *See*, Lynskey (n 18) 118-122.

59 GDPR, art 2.

60 *Puttaswamy* (n 16) (SA Bobde, J) [17].

2. The third country in question must have a means for ensuring a high level of protection that is effective in practice, in light of all the circumstances surrounding a transfer of personal data to a third country. This must include periodic checks as to whether the adequacy assessment is still justified and take into account all circumstances that have arisen after adoption of the decision.
3. Adequate protection must take into account the country's domestic law or international commitments.
4. Any system of self-certification must be reliable based on effective detection and supervision mechanisms enabling infringements of the rules, in particular the right to respect for private life and the protection of personal data, to be identified and punished in practice.
5. An adequacy decision must include a detailed explanation of how a country ensures an adequate level of protection.
6. There must not be limitations based on national security, public interest or law enforcement requirements that give third country law primacy over EU law.
7. Limitations must be placed on the power of public authorities (such as law enforcement authorities) to interfere with fundamental rights. In particular, any such access must be strictly necessary and proportionate to the protection of values such as national security, there must be clear and precise rules regarding the scope of application of a measure and for effective protection against the risk of abuse of data, and derogations and limitations in relation to data protection should apply only when strictly necessary.
8. Third country legislation must not authorise, on a generalised basis, storage of all the personal data transferred without any differentiation, limitation or exception being made in light of the objective pursued and without an objective criterion being laid down to determine the limits to the data, and its subsequent use, for purposes which are specific, strictly restricted and capable of justifying the interference entailed by access to that data and its use.[61]

In *Schrems II*, the Court of Justice emphasised in particular the following factors: (1) individuals must have effective and enforceable rights with regard to misuse of their personal data transferred;[62] (2) any bulk collection of data (such as in surveillance programs for national security purposes) must reflect

---

[61] Kuner, 'Article 45', in Christopher Kuner, Lee A Bygrave, and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (OUP 2020) 771, 781-782.

[62] *Schrems II* (n 21) [181].

the principle of proportionality;[63] and (3) as a specification of the first factor, there must be the possibility for individuals to bring actions to an independent and impartial court to have access to their personal data or to have them rectified or erased.[64]

In addition to these pronouncements of the Court of Justice, the DPAs have also laid out the main principles that must be contained in the law of a third country in order for it to be found adequate, which is important in light of the key role they play in interpreting the GDPR.[65] Thus, the former Article 29 Working Party (the predecessor to the EDPB) found that a third country must contain the following substantive protections:[66]

1. Basic data protection concepts or principles (personal data, data controller, sensitive data, etc.).
2. Grounds for lawful and fair processing for legitimate purposes.
3. The purpose limitation principle.
4. The data quality and proportionality principle.
5. The data retention principle.
6. The security and confidentiality principle.
7. The transparency principle.
8. The right of access, rectification, erasure and objection.
9. Restrictions on onward transfers.

The Working Party also enunciated procedural and enforcement mechanisms that such system must contain:[67]

1. A competent independent supervisory authority.
2. The data protection system must ensure a good level of compliance.
3. Accountability (i.e., obliging data controllers and/or those processing personal data on their behalf to comply with it and to be able to demonstrate such compliance in particular to the competent supervisory authority).

---

63 ibid [184].

64 ibid [194].

65 *See*, GDPR, art 70(e), charging the EDPB with examining questions covering application of the GDPR and issuing guidelines, recommendations and best practices to encourage its consistent application.

66 Article 29 Working Party, 'Adequacy Referential (updated)' (WP 254, 28 November 2017). *See also*, Kuner, 'Article 45' (n 61) 788.

67 Article 29 Working Party (n 66) 8. *See also*, Kuner, 'Article 45' (n 61) 789.

4. Providing support and help to data subjects in the exercise of their rights and appropriate redress mechanisms.

The EDPB has given further guidance on what constitutes 'essential guarantees' for third country surveillance measures as required by the Court of Justice in *Schrems II* with regard to both adequacy decisions and appropriate safeguards. These include the following principles: (1) processing must be based on clear, precise, and accessible rules; (2) there must be necessity and proportionality with regard to the legitimate objectives pursued; (3) there must be an independent oversight mechanism; and (4) effective remedies must be available for the individual.[68]

It can be seen that these requirements set a high standard for any third country to attain in order to receive an adequacy decision from the EU. They have been codified in Article 45(2) of the GDPR, which sets out the criteria the Commission must examine, when assessing the adequacy of protection in a third country. As the CJEU stated in its *Schrems I* judgment, the Commission's discretion with regard to evaluating the adequacy of protection ensured by a third country "is reduced", and review of the requirements stemming from EU data protection law and the Charter should be "strict".[69]

Two further points are important with regard to the standards that third country law must satisfy. First of all, the level of examination by the EU of third country law is quite detailed. For example, in *Opinion 1/15*[70] the CJEU found that a proposed international agreement between the EU and Canada to provide a legal basis for the transfer of airline passenger record ('PNR') data could not be concluded in its current form since it did not respect fundamental rights. In doing so, it objected to use of the term "etc." in one heading of the Annex to the Draft Agreement referring to PNR data elements, which read "Available frequent flyer and benefit information (free tickets, upgrades, etc.)".[71] The Court is thus willing to examine the wording even of an international treaty in minute detail in order to ascertain whether it ensures adequate protection, which shows that the EU's strict data protection standards help determine its degree of openness towards other legal orders.[72]

A second point is that EU institutions charged with evaluating third countries data protection standards such as the Commission and the EDPB may not always be aligned when it comes to the details of how they are to be evaluated.

---

68 EDPB, 'Recommendations 02/2020' (n 25) 8.

69 *Schrems I* (n 27) [78].

70 *Opinion 1/15*, Opinion of 26 July 2017 [2017] (Grand Chamber) (ECLI:EU:C:2017:592).

71 ibid [157].

72 *See*, Oreste Pollicino and Marco Bassini 'Bridge is Down, Data Truck Can't Get Through…A Critical View of the Schrems Judgement in the Context of European Constitutionalism' in Giuliana Ziccardi Capaldo (ed), *The Global Community: Yearbook of International Law and Jurisprudence 2017* (OUP 2017) 262.

These differences can be explained by the different natures of these institutions (the Commission being the executive branch of the EU, and the EDPB being an independent body comprised of European data protection authorities) and their different mandates (the Commission having to take both free trade and fundamental rights into account, and the EDPB being charged with ensuring consistent application of the GDPR). An example of this can be seen in divergences between the approaches of the Commission and the EDPB to the use of SCCs and other appropriate safeguards to transfer data in light of the *Schrems II* judgment. In the SCCs, the Commission has provided that parties using them must warrant that they have no reason to believe that the laws of third countries applicable to the processing would prevent the data importer from fulfilling its obligations under the SCCs.[73] The SCCs require that in providing the warranty, the parties must declare that they have taken due account of, among other things, "any relevant practical experience with prior instances, or the absence of requests for disclosure from public authorities received by the data importer for the type of data transferred."[74] However, in its Recommendations 01/2020, the EDPB states that the assessment of the parties with regard to the legal framework governing access to personal data by public authorities in a third country must be based "first and foremost on legislation publicly available".[75]

D. The difficulty of comparing data protection systems

The evaluation of third country standards under EU data protection law implies a comparison of third country law with EU law to see if the former is essentially equivalent to the latter. While the CJEU has always maintained that its mandate runs only to evaluating EU law and it cannot express a view on third country law and practice,[76] the need to review third country law is logically inherent in the evaluation of whether such law provides protection essentially equivalent to that under EU law.[77]

This raises an important question — while EU law provides the legal standard for comparison, how is the comparison to be conducted? The evaluation of whether a third country's law meets EU standards requires answers to a host of detailed questions, such as the following: what legal sources are to be compared (legislation, court decisions, etc.)? What role should practice (both administrative practice in public authorities, and the practice of data protection in the private sector) play, and by what method will evidence of it be

---

[73] European Commission (n 53) cl 14(a).

[74] ibid cl 14(b)(ii).

[75] EDPB, 'Recommendations 01/2020' (n 25) 14.

[76] *See*, eg, Opinion of Advocate General Mengozzi in *Opinion 1/15* (ECLI:EU:C:2016:656) [163].

[77] *See*, Kuner, 'International Agreements, Data Protection, and EU Fundamental Rights on the International Stage: Opinion 1/15 (*EU-Canada PNR*)' (2016) 55 Common Market Law Review 857, 879-880.

collected? How can those conducting the evaluation avoid cultural bias? How are differences in translation of legal texts taken into account? Scholars of comparative law have pointed out the risks of comparing legal systems, such as language and translation difficulties, misunderstandings caused by applying terms and concepts from domestic law to foreign systems, and differences between the law in the books and actual legal practice,[78] and it is not clear how the EU avoids these risks. In their classic work on comparative law, Zweigert and Kötz despaired of it ever being possible to define a general systematic method for conducting comparative legal research, and concluded that, in the end, it is necessary to rely largely on common sense and inspiration.[79] However, recourse to factors such as these may mean different things to different people and holds the risk of bias.

The EU seems to have given little thought to the methodological difficulties of determining adequacy. Documents concerning the Commission's deliberations about adequacy, including academic studies carried out on its behalf, have typically not been made public, and there is a lack of transparency concerning the entire procedure. For their part, the DPAs, who must provide the Commission with an opinion on a proposed adequacy decision[80] and thus play an important role in the procedure, have discussed adequacy in terms of the content principles that third country law must contain,[81] but have not gone into the details of how the adequacy assessment should be conducted, beyond saying that they should be provided by the Commission with all relevant documentation.[82] The CJEU has discussed the substantive requirements for adequacy in its two *Schrems* judgments, but has not provided guidance about the conditions under which such determination is to be carried out.

Comparing systems of fundamental rights to determine if one is essentially equivalent to the other is particularly difficult, since fundamental rights are inevitably tied up with cultural and historical factors. In addition, EU law has arisen in a unique constitutional and institutional context,[83] which makes it hard to develop a rigorous and objective comparative method for adequacy assessments. Renteln has argued that objective comparison of human rights systems must be based on an evaluation of cross-cultural, universal values for which a consensus exists, which in turn requires empirical research to identify

---

78 *See*, Basil Markesinis, *Comparative Law in the Courtroom and Classroom* (Hart 2003) 214-215; Rudolf Schlesinger, *Comparative Law* (4th edn, Foundation Press 1980) 815-836.

79 *See*, Konrad Zweigert and Hein Kötz, *Einführung in die Reichtsvergleichung auf dem Gebiet des Privatrechts*, vol 1 (JCB Mohr 1984) 33.

80 GDPR, art 70(1)(s).

81 Article 29 Working Party (n 66) 3.

82 ibid 4.

83 *See*, eg, Allan Rosas and Lorna Armati, *EU Constitutional Law: An Introduction* (Hart Publishing 2012, Kindle edition) 4.

such values.[84] Anecdotal evidence suggests that the EU does not use this approach in its adequacy negotiations. For example, a representative of a third country government told the author that in discussions with the Commission on an adequacy decision, the working method of the Commission representatives was to compare an English translation of the country's data protection legislation word-for-word with the text of the GDPR. However, as the CJEU has stated,[85] the protection of personal data requires not just a sufficient legal framework, but also protection in practice, and comparing the text of legislation cannot reveal how data protection actually operates 'on the ground'.

Tools for comparing human rights concepts such as the rule of law across different countries have begun to be developed,[86] but they are not yet granular enough to take into account the factors required for adequacy under the GDPR. Some scholars have compared data protection systems across different regions,[87] but they have not focused on a detailed comparison with EU data protection law in the context of adequacy determinations. Thus, EU adequacy decisions are beset with questions concerning their methodology and transparency.

These factors mean that third countries should not assume that the EU will conduct a fully informed evaluation of its legal system in deciding whether or not to issue an adequacy decision. In order to present its system as fully and accurately as possible, the third country should examine the criteria for adequacy listed in Article 45(2) of the GDPR and those identified by the CJEU, and be prepared to explain in detail how it meets them. In doing so, it should draw on the totality of its systems of law and public administration and how they function in practice to explain, as stated in the Commission's adequacy decision for Japan (another country like India that differs substantially from the EU in its legal and cultural background), "whether, through the substance of privacy rights and their effective implementation, supervision and enforcement, the foreign system as a whole delivers the required level of protection".[88] This must go beyond data protection legislation and also encompass consideration of factors such as constitutional protection, treaty protection, human rights institutions, civil law protection, criminal law and administrative laws, and

---

84 Alison Dundes Renteln, *International Human Rights: Universalism Versus Relativism* (Quid Pro Books 2013, Kindle edition) 115.

85 *Schrems I* (n 27) [74]; *Schrems II* (n 21) [137]; *Opinion 1/15* (n 70) [134].

86 *See*, eg, the Rule of Law Index published annually by the World Justice Project, which in its 2020 version compared the rule of law across 128 countries around the world. World Justice Project, 'WJP Rule of Law Index 2020' (WJP) <https://worldjusticeproject.org/our-work/research-and-data/wjp-rule-law-index-2020> accessed 11 May 2021.

87 For example, Graham Greenleaf, *Asian Data Privacy Laws: Trade and Human Rights Perspectives* (OUP 2014), which includes a chapter on privacy and data protection in India.

88 Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information, [2019] OJ L76/1, recital 3.

self-regulation.[89] Moreover, it is important to examine how these factors actually work in practice in the third country.

E. The law and politics of adequacy

The standards for adequacy decisions by the Commission are set by legal criteria, but the conditions for deciding whether to begin the process of issuing one, and ultimately the details of the final decision, are subject to political variables. The EU is required to uphold and promote its "interests"[90] and safeguard its "fundamental interests",[91] and this applies to data protection as well. The role that the EU's interests play in adequacy decisions can be seen in a statement by the Commission issued in 2017, which lists among the criteria for adequacy decisions, "the extent of the EU's (actual or potential) commercial relations with a given third country, including the existence of a free trade agreement or ongoing negotiations" and "the overall political relationship with the third country in question, in particular with respect to the promotion of common values and shared objectives at international level".[92] The Commission specifically mentions India in this regard, noting that it will engage in discussions with that country regarding an adequacy decision, depending on "progress towards the modernisation of its data protection laws".[93]

As confirmed by the statement in the Commission Communication quoted above, the EU puts particular emphasis on reaching adequacy decisions for countries with which it already has a free trade agreement in place, or with which it is in the process of negotiating one. This seems to be for practical (since much trade necessarily involves the flow of personal data), fundamental rights (since under a free trade agreement more personal data will flow to the third country), and political reasons (since issuance of an adequacy decision can improve relations with the country). An example of the political relevance of adequacy decisions can be seen in the EU adequacy decision for Japan, which mentions international trade several times.[94]

There is nothing wrong *per se* with politics playing a role in adequacy decisions, since law and politics can be viewed as 'structurally coupled systems',[95]

---

89 *See*, Greenleaf (n 87) 53.

90 Consolidated Version of the Treaty on European Union (TEU), [2012] OJ 2012 C326/13, art 3(5).

91 ibid art 21(2)(a).

92 European Commission, 'Communication from the Commission to the European Parliament and the Council, Exchanging and Protection Personal Data in a Globalised World', COM (10 January 2017), 8.

93 ibid. *See also*, Svetlana Yakovleva and Kristina Irion, 'Pitching Trade against Privacy: Reconciling EU Governance of Personal Data Flows with International Trade' (2020) 10 International Data Privacy Law 201, 218-220.

94 Commission Implementing Decision (EU) 2019/419 (n 88) recitals 1 and 190.

95 Anne Peters, 'Compensatory Constitutionalism: The Function and Potential of Fundamental International Norms and Structures' (2006) 19 Leiden Journal of International Law 579, 609.

and the decisions the EU takes concerning adequacy must be a result of political calculations. However, third countries should realise that their negotiations on an adequacy decision may become entangled with unrelated political factors,[96] and that such negotiations may create political tensions.[97]

III. THE GDPR AND THE WAY FORWARD FOR INDIA

A. EU data protection standards and India

The EU's adequacy standard for data transfers has a direct impact on India, both with regard to the issuance of an adequacy decision and the use of appropriate safeguards like the SCCs.

India originally sought an adequacy decision as early as 2009,[98] but these efforts failed to bear fruit, and initial talks over a free trade agreement were suspended. However, the EU has stated that it "remains committed to working towards an ambitious, comprehensive and balanced agreement FTA [sic] with India that responds to each side's key interests and is a win-win",[99] and it seems that India is set to resume talks on a free trade agreement with the EU.[100] In the scope of these discussions, India has apparently also renewed its bid to obtain an adequacy decision, which would be reciprocal (i.e., if successful it would also involve India finding that EU law was adequate based on Indian standards).[101]

---

[96] For example, in 2010 the government of Ireland delayed an EU adequacy decision for Israel based on alleged Israeli government involvement in the forging of Irish passports. *See*, Jon Ihle, 'Ireland blocks EU data sharing with Israel' *Jewish Telegraph Agency* (Dublin, 8 July 2010) <http://www.jta.org/2010/07/08/news-opinion/world/ireland-blocks-eu-data-sharing-with-israel> accessed 16 May 2021. Israel later received an adequacy decision from the European Commission. Commission Decision 2011/61/EU of 31 January 2011 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the State of Israel with regard to automated processing of personal data, [2011] OJ L27/39.

[97] *See*, eg, Jennifer Stoddart, Benny Chan and Yann Joly, 'The European Union's Adequacy Approach to Privacy and International Data Sharing in Health Research' (2016) 44 Journal of Law, Medicine & Ethics 143 (concerning tensions with Quebec concerning adequacy).

[98] *See*, Graham Greenleaf, 'India's U-Turns on Data Privacy' (2011) UNSW Law Research Paper 2011-42, 19 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1964013#> accessed 17 May 2021.

[99] European Commission, 'EU-India Trade Negotiations' (European Commission, 22 April 2020), <https://ec.europa.eu/trade/policy/countries-and-regions/countries/india/> accessed 17 May 2021.

[100] Business Standard, 'India Set to Resume Talks on Free Trade Agreements With EU, US' *Business Standard* (New Delhi, 21 November 2020) <https://www.business-standard.com/article/economy-policy/india-set-to-resume-talks-on-free-trade-agreements-with-eu-us-120112100594_1.html> accessed 17 May 2021.

[101] *See*, Megha Mandavia, 'India to Approach the EU Seeking "Adequacy" Status with the GDPR' *The Economic Times* (30 July 2019) <https://economictimes.indiatimes.com/internet/india-to-approach-the-eu-seeking-adequacy-status-with-the-general-data-protection-regulation/articleshow/70440103.cms> accessed 19 May 2021. The Commission adequacy decision for

It is worthwhile for India to strive for an adequacy decision because of its close economic ties with the EU, the ongoing efforts to conclude a trade agreement, and the positive signal that successful negotiations would send about the standard of protection in India's data processing industry. However, the road towards such a decision is likely to be difficult, and, as will be explained below, could be facilitated if India were to broaden its ambitions and seek to meet international standards for data protection as well as those of the EU.

In the past, it seemed certain that the level of protection provided by Indian law would not meet EU standards,[102] but the recognition of a right to privacy at the constitutional level by the Supreme Court of India in its *Puttaswamy*[103] decision has removed an important impediment to an adequacy finding. However, as the Supreme Court noted, privacy and data protection are not synonymous, with privacy covering "intimate matters to which a reasonable expectation of privacy may attach", while data protection is a broader concept that is related to the protection of one's identity[104] and that is to be implemented by the State "after a careful balancing of the requirements of privacy coupled with other values which the protection of data sub-serves together with the legitimate concerns of the State".[105] This implies that the recognition of a right to data protection would require further legislative action, and the Supreme Court commended to the government "the need to examine and put in place a robust regime for data protection".[106] Thus, although the judgment may not have identified an existing right to data protection, it did mention the need to implement such right through the enactment of legislation.

On December 11, 2019, the Indian government proposed the Personal Data Protection Bill 2019 (the Bill),[107] which evidences the influence of the GDPR and references a number of concepts that are central to it (including the prohibition of data processing, data quality, sensitive data, the creation of a data protection authority, the right to be forgotten, and others). However, the Bill

---

Japan was also a reciprocal decision. *See*, Commission Implementing Decision (EU) 2019/419 (n 88) annex 1.

[102] *See*, Greenleaf, *Asian Data Privacy Laws* (n 87) 432.

[103] *See*, *Puttaswamy* (n 16), in which the Court stated at that "Privacy is a constitutionally protected right which emerges primarily from the guarantee of life and personal liberty in Article 21 of the Constitution. Elements of privacy also arise in varying contexts from the other facets of freedom and dignity recognised and guaranteed by the fundamental rights contained in part III".

[104] ibid [177].

[105] *Puttaswamy* (n 16) [179].

[106] ibid.

[107] Personal Data Protection Bill (n 20).

has been criticised, both in India[108] and by international experts,[109] as falling short of the necessary standards, and even as providing a legal basis for future violations of privacy. Just a few of the problematic provisions that would prevent it from meeting the standards of the GDPR include the unrestrained power given to the government to exempt its agencies from the Bill's application;[110] a broad exemption for Indian outsourcing companies processing the data of foreigners;[111] and concerns that the Bill's provisions establishing a DPA would not result in it being truly independent.[112]

Apart from the apparent deficiencies of the Bill, the recent history of data processing in India is replete with schemes that have adverse effects on privacy, such as initiatives to promote data localisation,[113] the issuance of biometric ID cards to the entire population (the Aadhaar card project),[114] and the widespread use of facial recognition technology without sufficient privacy protections.[115] Phenomena such as these have led to claims that India is becoming a surveillance state.[116] Large-scale data collection could also facilitate access to data by the intelligence and security services, which already seems to be happening in India.[117]

---

[108] *See*, eg, Megha Mandavia, 'Personal Data Protection Bill Can Turn India into "Orwellian State": Justice BN Srikrishna' *The Economic Times* (12 December 2019) <https://economictimes.indiatimes.com/news/economy/policy/personal-data-protection-bill-can-turn-india-into-orwellian-state-justice-bn-srikrishna/articleshow/72483355.cms> accessed 21 May 2021.

[109] *See*, Graham Greenleaf, 'India's Personal Data Protection Bill, 2019 Needs Closer Adherence to Global Standards' (2020) Submission to Joint Committee, Parliament of India <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3539432> accessed 21 May 2021.

[110] Personal Data Protection Bill (n 20) cl 35.

[111] ibid cl 37.

[112] ibid ch IX.

[113] *See*, Anupam Chander and Uyên P Lê, 'Data Nationalism', (2015) 64 Emory Law Journal 677, 694-696; Arindrajit Basu, Elonnai Hickok and Aditya Singh Chawla, 'The Localisation Gambit: Unpacking Policy Measures for Sovereign Control of Data in India' (The Centre for Internet and Society, 19 March 2019) <https://cis-india.org/internet-governance/resources/the-localisation-gambit.pdf> accessed 21 May 2021.

[114] For criticism of the Aadhaar scheme, *see*, Graham Greenleaf, 'Your Money or Your Life? Modi's Deceptive Enactment of India's ID Legislation' (2016) UNSW Law Research Paper No 2016-53 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2800835> accessed 22 May 2021; Vrinda Bhandari and Renuka Sane, 'A Critique of the Aadhaar Legal Framework' (2019) 31 National Law School of India Review 72. On 26 September 2018, the Supreme Court of India upheld most of the provisions of the Aadhaar scheme in *KS Puttaswamy v Union of India* (2019) 1 SCC 1 <https://sflc.in/updates-aadhaar-final-hearing/aadhaar-judgement>.

[115] *See*, Smitri Parsheera, 'Adoption and Recognition of Facial Recognition Technologies in India: Why and Why Not?' (2020) Data Governance Network Working Paper 05, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3525324&download=yes> accessed 25 May 2021.

[116] *See*, Ananth Padmanabhan and Vasudha Singh, 'The Aadhaar Verdict and the Surveillance Challenge' (2019) 15 Indian Journal of Law & Technology <http://ijlt.in/wp-content/uploads/2020/07/Aadhar-verdict.pdf> accessed 25 May 2021.

[117] *See*, Smirti Parsheera and Prateek Jha, 'Cross-Border Data Access for Law Enforcement: What Are India's Strategic Options?' (Carnegie India, 23 November 2020) <https://carnegieindia.org/2020/11/23/cross-border-data-access-for-law-enforcement-what-are-india-s-strategic-options-pub-83197> accessed 25 May 2021; Sunil Abraham, 'Systematic Government Access

Indian law in areas such as anti-terrorism and money laundering may also require that access to the data be given to Indian law enforcement authorities in a way that could violate the standards of the GDPR. For example, under the Prevention of Money Laundering Act,[118] financial institutions and payment system operators operating in India must furnish information about suspicious transactions to the Indian Financial Intelligence Unit,[119] which may require them to transfer personal data stored in the EU to the Indian authorities. While analysing the issues this raises would exceed the bounds of this article, suffice it to say that under the GDPR, non-EU legal requirements to transfer personal data to a third country may only be recognised if they are based on an international agreement with the EU or a Member State.[120] This means that in this situation, there will usually be no legal basis under the GDPR for transferring the data to authorities in India, which could put companies in a conflict of laws situation.

A significant issue that goes beyond data protection is the lack of horizontal enforcement of the right to privacy under *Puttaswamy*, i.e., the fact that the right is only enforceable against the State and not against private entities such as companies.[121] Nowadays, the distinction between public and private processing of personal data is increasingly blurred, as public entities often seek to process personal data originally collected by the private sector (e.g., PNR or airline passenger data, financial data, and many other types).[122] Limiting the scope of constitutional rights to violations by State entities can reduce their efficacy, and has been the subject of criticism in India in recent years.[123] The lack of sufficient controls on government access to private-sector data is a particular concern with regard to a potential EU adequacy decision, since this was one of the factors that caused the CJEU to invalidate the Privacy Shield in its *Schrems II* judgment. One therefore hopes that in the future, the Supreme Court of India will expand the scope of the right to privacy to include violations by private actors as well.

---

to Private-Sector Data in India' in Fred H Cate and James H Dempsey, *Bulk Collection: Systematic Government Access to Private-Sector Data* (OUP 2017).

118 Prevention of Money Laundering Act 2002.

119 ibid cl 2.17.

120 GDPR, art 48.

121 *See*, Sreekar Aechuri, 'Horizontal Applicability of the Right to Privacy in India' (2019) South Asia Journal <http://southasiajournal.net/horizontal-applicability-of-the-right-to-privacy-in-india/> accessed 26 May 2021.

122 *See*, Fred H Cate and James H Dempsey, 'Introduction and Background' in Fred H Cate and James H Dempsey, *Bulk Collection* (n 117) xxviii, stating that there has been a growing worldwide trend toward government access to private sector data.

123 *See*, eg, Siddharth S Aatreya, 'Private Governments and the Indian Constitution — Rethinking "State" under Article 12' (*NLSIR Online*, 25 July 2019) <https://nlsir.com/private-governments-and-the-indian-constitution-rethinking-state-under-article-12/> accessed 26 May 2021.

These examples indicate that, while India has made great strides in recent years in recognising privacy as a right at the constitutional level, it still falls short on the level of adopting adequate legislative standards and of implementing data protection in practice. Thus, without going into further detail, it can be assumed that the Bill in its current form would not satisfy the standards of the GDPR, and that India would likely not be declared by the Commission to provide an adequate level of protection as matters currently stand.

B. The role of international data protection standards

Besides the enactment of strong data protection legislation, recognising international standards and becoming involved in the work of those international organisations that promulgate them could also play an important role in strengthening India's own standards. This is important because data protection is a topic of international significance that goes beyond the GDPR. It could also help make the Indian government more aware of the implications of enacting legislation that may produce conflicts with foreign data protection legislation.

In *Puttaswamy*, the Indian Supreme Court emphasised that "the recognition of privacy as a fundamental constitutional value is part of India's commitment to a global human rights regime."[124] Among the international instruments the Supreme Court examined in its *Puttaswamy* judgment was the European Convention on Human Rights ('ECHR'),[125] which is the major treaty of European human rights law adopted under the auspices of the Council of Europe,[126] and is not an instrument of EU law but is closely connected with it.[127] The GDPR also includes interfaces with both the ECHR[128] and the data protection treaty adopted by the Council of Europe, namely the Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Convention 108,[129] which has recently been modernised[130]). Convention 108 is the only legally binding multilateral treaty dealing specifically with data protection, and adherence to it is recognised as an indication as to whether third

---

[124] *See*, *Puttaswamy* (n 16) 126.

[125] European Convention for the Protection of Human Rights and Fundamental Freedoms, September 3, 1953, ETS 5, 213 UNTS 221.

[126] The Council of Europe is an international human rights organisation that is not an entity of the European Union but works closely with it. *See*, <https://www.coe.int/en/web/about-us/who-we-are> accessed 26 May 2021.

[127] For example, art 52(3) of the Charter requires that the meaning and scope of rights under it shall be the same as under the ECHR, and the rights enshrined in the ECHR constitute general principles of EU law (TEU (n 90) art 6(3) and *Schrems II* (n 21) [98]).

[128] *See*, GDPR, recital 73, stating that restrictions on data protection rights under GDPR, art 23 should be in accordance with the ECHR.

[129] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, opened for signature on 28 January 1981, in force 1 October 1985, ETS 108.

[130] Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, opened for signature on 10 October 2018, CETS No 223.

country law meets EU legal standards for data protection (for example, under the GDPR, a third country's accession to the Convention 108 should be "taken into account" by the Commission when assessing adequacy[131]).

International data protection standards such as those under the Modernised Council of Europe Convention 108 could play an important role as India implements a legislative regime for data protection. Aligning Indian data protection law with international standards could help boost the chance of India receiving an adequacy finding from the EU. In addition, India could become involved in the work of the Council of Europe, as a way to make contacts with other governments interested in data protection, showcase its own interest in the topic, and gain insights that could help it better structure its legislation to meet international standards. For example, India could apply to participate as an observer in the work of the Council of Europe's Consultative Committee on data protection,[132] which typically welcomes participation in its work by observer States. Becoming involved in the work of the Committee could also help the Indian government decide whether it should consider acceding to the modernised Convention 108 (Article 27 of the Convention foresees accession by non-member States of the Council of Europe, and several have already signed it, including Argentina, Mauritius, Tunisia, and Uruguay).[133]Accession to the Convention would be a powerful signal of India's commitment to data protection and would increase the chances of receiving an adequacy decision.

Another important international policymaking forum that deals with data protection is the Organisation for Economic Co-Operation and Development ('OECD'). Since being originally adopted in 1980[134] and then modernised in 2013,[135] the OECD's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, while not legally-binding, have provided an influential international baseline for States as they enact privacy legislation. India is already a 'key partner' of the OECD and collaborates with it on many initiatives,[136] and the author has learned that India has been invited to participate in the work of the OECD's Committee on Digital Economy Policy (CDEP). Participation in the data protection work of the OECD could prove useful to India in making contacts, building knowledge, and explaining its approach to privacy and data protection to the wider world.

---

131 GDPR, recital 105.

132 *See*, <https://www.coe.int/en/web/data-protection/consultative-committee-tpd> accessed 28 May 2021, for information on the work of the Committee.

133 *See*, <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223/signatures> accessed 28 May 2021.

134 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980) <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm> accessed 29 May 2021.

135 The OECD Privacy Framework (2013) <http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf> accessed 29 May 2021.

136 *See*, OECD, 'Active with India' (2019) <https://issuu.com/oecd.publishing/docs/active-with-india-2019?fr=sNmM1ODkzNTk1MQ> accessed 31 May 2021.

C. Conclusions

The GDPR and the *Schrems II* judgment create uncertainties and opportunities for both the EU and a large third country like India that has a tradition of the rule of law but not a history of data protection. For the EU, the judgment requires it to set a high standard for its data transfer mechanisms, including both adequacy decisions and appropriate safeguards such as SCCs. The standard set by the judgment also creates uncertainties about how the comparative method used for adequacy decisions can cope with assessing the legal system of a country like India that is highly complex and culturally quite different from the EU.

From India's point of view, orienting its data protection standards around the GDPR would have several advantages. The GDPR has become the premier legal standard for data protection and using it as the basis for India's data protection legislation would help ensure that it provides a high level of protection. Indian IT companies have many customers in the EU such that basing its standards on the GDPR could bring economic benefits. In addition, data protection can play an important role in the protection of fundamental rights in general, by protecting the participation of individuals in social relations, safeguarding other rights such as freedom of expression, preventing unfair discrimination, and promoting fairness in decision-making processes.[137] Thus, enacting strong data protection legislation could bring societal benefits to India.

As the Supreme Court of India has recognised, India's international legal commitments are of particular significance as the country moves to enact data protection legislation. The growing recognition of data protection around the world means that India should look beyond the EU and also orient its data protection legislation around international standards, as well as become more involved in international organisations like the Council of Europe and the OECD that contribute to their development.

[137] *See*, Hustinx (n 2) 127.