INTERNATIONAL JOURNAL OF RESEARCH AND ANALYSIS VOLUME 5 ISSUE 3 ISSN 2347-3185 2018

INTERPLAY OF GATS AND GDPR (BALANCING TRADE AND NON-TRADE CONCERNS IN A DIGITALISED ERA)

*** ANJALI MENGHANI**

Concerns Regarding Transferring of Personal Data to Third Countries and International Trade

In this virtual world of digitalised trade, where the enterprises depend completely on collecting the personal data from the internet, the concerns regarding protection of data and privacy have become of considerable importance.[1] Since a significant part of information is stored on internet, both the information which is stored and the collected, has potential dangers of misuse.[2] The central issue in this case lies in the 'location' of the data, and the regulations regarding the same. As there are a few countries which are more open with regards to the cross-border flow of data while there are some that restrict the flow of data from one country to the other, in light of their data protection and privacy issues.[3] In view of *Sullivan* these restrictions are considered to be an 'indirect barrier' to the use of cloud and unnecessarily increases the cost, as in his research it was found that the use of cloud was cheaper in the U.S while in the EU, in order to comply with the data protection laws the users had to pay a premium.[4] Although, as much as it is important for the service providers to have the access to personal data for its growth and economic development, there has been a considerable misuse by the private sector of the personal data so provided, and hence, in this globalised scenario, one of the major international concern is regarding data protection and privacy rights in a digitalised age[5] and the EU regime on transferring the data are driven by these policy objective factors.[6]

[1] Diane A. MacDonald and Christine M. Streatfeild. 'Personal Data, Privacy and The WTO'. (2014) 36 Houston Journal of International Law. p 626

[2] Tara J. Radin 'The Privacy Paradox' (2001) 20 Business and Professional Ethics Journal. p146.

[3] For instance, The EU tends to be more protective when it comes to the protection of data and the privacy rights of their citizens. By contrast, U.S tends to be more in favour of free flow of data.

[4] Laura K. Donohue, *The Future of Foreign Intelligence, Privacy and Surveillance in Digital Age* (Oxford University Press 2016)

[5] Kriangsak Kittichaisaree and Christopher Kuner, 'The Growing Importance of Data Protection in Public International Law' (EJIL: Talk! 2017) <https://www.ejiltalk.org/the-growing-importance-of-data-protection-in-public-international-law/> accessed 30 July 2017.

[6] W. Kuan Hon, *Data Localisation Laws and Policy* (Edward Elgar Publishing 2017).

In most of the international legal instruments privacy has been incorporated as a fundamental right[7] and particularly in the EU, privacy right plays a comparatively stronger role. Data protection standing as a separate right from that of privacy. GATS does not have any provision specifically dealing with the transfer of data and privacy issues, however, through the provision of General Exceptions embedded in GATS, it confirms that the important data related issues concerning trade could be addressed by the existing framework.[8]

The section briefly describes the recently enforced Data Protection Regime in the EU (owing to its stringent regime), in light of the enforced Data Protection Directive and gives a brief overview of the reforms and objectives of the proposed Regulation (GDPR). It also points out the minor changes introduced by GDPR in contrast with that of the DPD with regards to the international flow of data. Further, it seeks to discuss whether the same falls within the ambit of the agreement and its consistency with regards to GATS Obligations.

Data Localisation laws in EU and The Policy Objectives

Primarily, The EU Charter of Fundamental Rights stands as a legal footing to the Data Protection Rights in EU, it operates as one of the core mechanism which grants the right to protect data.[9] Apart from that, the Data Protection Directive[10] and the E-Privacy Directive[11] provided for a regulatory regime for protecting data. To promote and ensure the data protection rights of the citizens, the EU Commission has recently enforced an amended the regime by introducing the General Data Protection Regulation (the "Regulation" or "**GDPR**"), which replaced the previous and the abovementioned Directive. The Regulation promotes the free flow of data within the EEA Zone, having the least the minimum standards. However, such a free movement is only within the EU Zone and has different standards and criteria when the dealing with other countries. It establishes standards not only for compliance but also for the procedure to prove compliance.[12] However, while dealing with the cross-border transfer of data over the internet, often concerns have been raised regarding the protection of 'personal data' and privacy of the citizens. 'Personal Data' has been given a broad definition under Article 4(1) of GDPR, which is the information regarding any *'identifiable natural person'* and in terms of the transferring of data internationally, GDPR,

[7] Article 12, Universal Declaration of Human Rights. Article 8, European Convention for the protection of Human Rights and Fundamental Freedoms.
[8] Article XIV c(iii), GATS
[9] Article 7, Article 8 (1) (2) (3)
[10] Directive 95/46/EC
[11] Directive 2002/58/EC
[12] Article 5(2), GDPR

introduces restrictions, and the requirements to be met with respect to the transfer of personal data. The approach provided in GDPR, so far appears to be more stringent than the DPD, especially when it comes to transfers.[13] Reason being that it aims to serve a number of objectives, privacy and data protection being the prime one, which also lead to the application of rules on processing of data. Especially with respect to challenges affirming information security and protection of rights when non-EU countries are involved.[14] They further clarify the rules when dealing with the sensitive information, quality of data, confidentiality, right of data subjects and many more issues.[15]

- **Aspect of Extra-Territoriality in GDPR**

The GDPR does not completely denies the flow of data to and from the third countries. In light of Article 3(2), the Regulation, it is also applicable to the controllers that are not established within the EU, utilizing the equipment situated in the territory. The scope of extra-territoriality is considerably wider as it attracts the third countries for its application not only when they are offering goods and services but also when there is a monitoring behaviour in the service.[16] For instance, if a company situated in India, irrespective of having any subsidiaries in the EU, if its offering any kind of services online to the EU residents, in that case the GDPR would be applicable when in force. However, in this scenario the previously enforced DPD was not applicable. Hence, the GDPR is considered to be more broad in its extra-territoriality application.

- **International Flow of Data and The Changes Introduced by GDPR**

The Regulation has different standard(s) when the third countries are involved. Chapter V of the Regulation, prohibits the transferring the personal data to any third country(ies) where the standard for the regime is not of the adequate level. Essentially, the Directive validly qualifies the transfer of data to the third country only when the third country has the standard of data protection regime similar to that of EU.[17] These are the certain exemptions granted to the third countries when the transfer of data is considered.

[13] W. Kuan Hon, *Data Localisation Laws and Policy* (Edward Elgar Publishing 2017). p 13
[14] WP47
[15] Neil Robinson and others, 'Review of the European Data Protection Directive' (2017) p7 <https://ico.org.uk/media/about-the-ico/documents/1042349/review-of-eu-dp-directive.pdf>accessed 29 July 2017.
[16] W. Kuan Hon, *Data Localisation Laws and Policy* (Edward Elgar Publishing 2017).
[17] Article 25(1), DPD

It is of high relevance to note that until now, no third country has been categorised as inadequate while considering its standard of data protection. But, in Safe Harbour Agreement between the U.S and EU which provided for compliance of US companies with the Directive, reflects the level of adequacy required by the EU Commission. In 2015, the same agreement was held to be invalid by the ECJ in "*Maximillian Schrems v. Data Protection Commissioner".*[18] This decision has had a major impact on the data flows being transferred between the two countries as the transfer of this personal data is prohibited, consequently having a significant impact on the business and growth for both the countries.[19]

Therefore, it can be said that this provision indirectly imposes a restriction on the transfer of data to the countries those do not have an adequate level of data protection regime.[20]

Another exemption that is granted by the EU, is known as the *"appropriate safeguards".*[21] The provision is mostly similar to that of DPD, however, the certain changes introduced are like the safeguards may only be granted with or without the DPA authorisation depending on the scenarios.[22] Also, while conserving the third exemption with regards to derogations, changes have been considered in respect of:

a. Consent- When in contrast with DPD, under GDPR, the standard for a consent to be valid has been raised quiet high. As the consent has to be provided in a form that is legible and comprehensible and the purpose for processing data should also be provided with it. The form of the consent should use clear terms and language. It must also be easier to withdraw.
b. Penalties- The rules with regards to penalties have also been raised and varies from the types of infringements. Now, breach of GDPR regulations such as not having consent or violating privacy, violating restrictions on international transfer etc., could lead to a fine of up to 4% of the turnover.[23] The other category of fines includes for the breach of obligations of controllers or processors or other monitoring bodies, which could be fined up to 2% of annual turnover.

[18] C-362/14 2015:650

[19] Yi-Hsuan Chen, 'The EU Data Protection Law Reform: Challenges for Service Trade Liberalization and Possible Approaches for Harmonizing Privacy Standards into the Context of GATS' (2015) 19 Spanish Yearbook of International Law. p 214

[20] Neil Robinson and others, 'Review of the European Data Protection Directive' (2017) p33 <https://ico.org.uk/media/about-the-ico/documents/1042349/review-of-eu-dp-directive.pdf>accessed 29 July 2017.

[21] Article 46, GDPR

[22] Article 46(2), 46(3) and 46(4), GDPR.

[23] Article 83(5)

c. "Right to be Forgotten" – Following the *"Google Spain Case"*[24] this right has now been incorporated in the GDPR, although not as an absolute right.[25] It can be invoked in circumstances where there are absolutely no grounds for the controller to process the information.

We can conclude from all these changes that the rules under the GDPR are more stringent and onerous for the controller than those rules available in the DPD.

Interplay Between GATS Obligations and EU Regime on Data Protection and Privacy

- **GATS: Scope of Application**

The primary question that arises before considering the consistency of the measure is to deduct whether the measure adopted by the EU, that is, the said Regulation falls within the ambit of the Agreement.

Pursuant to Article I.2, as services is defined by its modes of supply, in this scenario, firstly, it is important to determine whether a supply of service is involved by any of the four modes.[26] The two regimes available for the classification of services under GATS are, *"The Services Sectoral Classification List"* and the *"UN Central Product Classification"* which provides for an inclusive list of service sectors and sub-sectors.[27] In the present situation, the activities pertaining to processing data are classified under the *"computer related services"* under CPC and the sub-sector of *"data processing services"* within the Sectoral Classification List. From the same reasoning it could be assumed that in this case, there is cross-border supply of service involved.[28]

Secondly, to note that the GDPR, i.e., the measures by the EU potentially falls within the scope of the Agreement as the said measures *"affects"* the international trade.[29] In *Canada-Autos* a similar issue was addressed wherein the distinction was made between *"trade in services"* and measure that *"affects"* the trade in services.[30]

By this reasoning, it could be deduced that the said measures by the EU falls within the Scope of the Agreement.

---

[24] *"Google Spain SL and Google Inc. v Agencia Espanola de Proteccion de Datis and Mrio Costeja Gonzalez."*
[25] Article 17
[26] Yi-Hsuan Chen, 'The EU Data Protection Law Reform: Challenges for Service Trade Liberalization and Possible Approaches for Harmonizing Privacy Standards into the Context of GATS' (2015) 19 Spanish Yearbook of International Law. p 214
[27] Rolf H Weber and Mira Burri, *Classification of Services in the Digital Economy*, (Springer 2013) ch II, p17.
[28] Yi-Hsuan Chen, 'The EU Data Protection Law Reform: Challenges for Service Trade Liberalization and Possible Approaches for Harmonizing Privacy Standards into the Context of GATS' (2015) 19 Spanish Yearbook of International Law. p214
[29] Article I.2, GATS
[30] WT/DS139/AB/R paras161-167

- **Potential GATS Violations: Consistency Tests**

As the measures fall within the Agreement, it is considerable to assess whether the said measure are in compliance with the GATS obligations, with respect to the MFN treatment or Market Access Obligations, or whether the same measures are WTO inconsistent.

a. MFN Treatment Obligations

This section analyses whether the upcoming EU regulatory regime on GDPR, with regard to transfer of data to third countries, provides exactly the similar treatment to each state to satisfy the GATS MFN obligations. The key concern here is, to establish whether the services in question are "like" services or not, as an MFN violation can only be established when the two services compared are "like services". Chapter V of GDPR, makes two references, one that deals with the services and service suppliers, one, from the country which has an adequate level Data Protection requirement and the other that does not, which seems to suggest that services in question here are the quiet the same, dealing with the processing of data services, otherwise the question of similar level of protection wouldn't have arose in the first place.

Since there exists the likeness of services, The GDPR, when dealing with transferring data to third countries. Pursuant to Article 42 of GDPR[31], referring to the certification mechanism with respect to transferring data to other countries or organisation, puts additional weights and costs upon the service providers, whose standards for protection of data is not equivalent to that of the EU regime.[32] It directly grants a favourable treatment to the members who have the similar standard as that of EU, and such a similar treatment is not accorded *"immediately or unconditionally"* to the other members.[33] The analysis concludes that with the enforcement of GDPR, there are potential violations of EU's MFN obligations under Article II, GATS.

b. Market Access Obligations

As previously established, there exists a general prohibition on imposing any kinds of restrictions in a sector in which the member has made market access commitments, unless the same restriction has expressly been specified in the Schedule of Commitments. When it

[31] Nicholas Vollmer, 'Article 42 (EU GDPR) (Privacy-Regulation.EU,2017) <http://www.privacy-regulation.eu/en/42.htm> accessed 1 August 2017.

[32] Yi-Hsuan Chen, 'The EU Data Protection Law Reform: Challenges for Service Trade Liberalization and Possible Approaches for Harmonizing Privacy Standards into the Context of GATS' (2015) 19 Spanish Yearbook of International Law. p216

[33] *Ibid*

comes to examining EU's Specific Schedule of Commitments, the market access commitments made by the EU in data processing sub-sector is "none". [34] Which means that there are no limitations on transferring personal data to other member nations that are expressly specified by the EU. And considering the consistency tests as discussed above, with coming in force of provisions like Article 41, 42 and 44 of the GDPR, would lead to a restriction of trade. Theoretically, leading to EU's in a potential violation of its GATS Obligations.[35] Having established the inconsistent measures of the members, the next issue to consider is whether these otherwise WTO-inconsistent measures could be justified by invoking the General Exceptions provision embedded in the GATS? And if yes, what are the standards and extent to which it could be justified. These questions have been dealt significantly in the next chapter. So, Article XX, GATT and Article XIV, GATS, are often referred to as the Balancing provisions in the Agreements. The objective of this chapter is to analyse the Panel and Appellate Body Reports with regards to the measures at stake discussed in the previous chapter and how are the same justified so far by invoking Article XIV of GATS. It also analyses the disputes that invoked Article XX, GATT and the lessons learnt from them. Lastly it attempts to make analysis on the potential dispute that may arise considering EU's stringent regime on transfer of personal data to third countries.

3.1 Legal Nature and Structure of the General Exception Provision in GATS

According to the analysis done by *Delimatsis*,[36] Article XIV, GATS, follows a model parallel to that of Article XX, GATT, providing an exhaustive list of exceptions that are of fundamental interests to the society. Following a similar structure and terminology, the Appellate Body permits the application of informative interpretation of the jurisprudence under Article XX. That is, for justifying the measures so inconsistent, an equivalent two-tier test has been transferred into GATS.[37] However, irrespective of the textual similarities, there exists a few differences between the two agreements, for instance, in Article XIV, seeks to protect both the public morals and public order, whereas, GATT, focuses only on protecting

[34] 'WTO | European Union – Member Information' (Wto.org, 2017) <https://www.wto.org/english/thewto_e/countries_e/european_communities_e.htm#members_may04 > accessed 1 August 2017.

[35] Yi-Hsuan Chen, 'The EU Data Protection Law Reform: Challenges for Service Trade Liberalization and Possible Approaches for Harmonizing Privacy Standards into the Context of GATS' (2015) 19 Spanish Yearbook of International Law. p218

[36] Panagiotis Delimatsis, 'Don't Gamble with GATS- Interaction Between Articles VI, XVI, XVII and XVIII GATS, In the Light of the US-Gambling Case' (2006) 40 Journal of World Trade. p1059-80

[37] The World Trade Organisation, Law Practice and Policy. Third Edition. 2015. Mitsuo Matsushita, Thomas J. Schoenbaum, Petros C. Mavroidis, Michael Hahn. Page 614.

the public morals interests[38], this shows that the same provision has been interpreted in a broad sense as it leads to the finding that "public order" is also considered of fundamental interests to the society.[39] However, the scope of the same provision is narrowed down, as a special emphasis has been added that in order to justify the grounds on maintaining public order,[40] there has to be a serious threat to the fundamental interests of the society, which gives a clear picture that demanding standards of this provision has to be met in order to invoke this provision.[41] These deviations could only be allowed if it satisfies the two-tier test, relating to the *"necessity"* and fulfilling the requirements of *"The Chapeau"*. The same has been interpreted by the DSB in the cases invoking the general exception clause and has been discussed in detail below. Further, this chapter also seeks to analyse the justification of the grounds on which the EU could invoke this provision, in an event of a potential dispute with regards to its inconsistent measures.

EU Legal Framework on Data Protection and Privacy: Justification by Article XIV

As noted previously, the inconsistency of the EU's framework on the Data Protection and Privacy, with regards to its market access and most favoured nation treatment obligations. In an event of any possible dispute, for EU the next thing to evaluate would be as to whether the said measures could be justified by GATS. In the present issue at stake, the first thing to consider is whether the said non-trade concern, i.e., the protection of personal data and privacy, falls within the exhaustive list of Article XIV.

- **The Necessity Requirement**

To prove that the measure undertaken by the Member is justified by the said exception clause, the primary question is to know is whether it could be categorised within the exhaustive list provided by Article XIV. The data protection and privacy exception falls under Article XIV(c)(ii), however, the only data that could fall within the article is only that is confidential. That is, only when the information is confidential or private could it fall within the exceptions to justify. Until this date, this provision dealing with the privacy and other exceptions have not been invoked. The standards for determining necessity is relied on a number of factors as discussed above and such a balancing test needs to consider the

[38] Article XIV, fn 5
[39] Mira Burri and Thomas Cottier, *Trade Governance in Digital Age: World Trade Forum.* (Cambridge University Press 2012) pt III, ch 11, p283.
[40] Article XIV, fn 5, GATS
[41] Mira Burri and Thomas Cottier, *Trade Governance in Digital Age: World Trade Forum.* (Cambridge University Press 2012) pt III, ch 11, p283, para 1.

potential threat to the values, how restrictive effect will it have on the trade and if there's any other alternative which could be WTO consistent.[42]

Going by the EU Charter on Fundamental Rights encompasses the protection of privacy and personal data and has been given a high level of importance and therefore the said regulation establishes provisions dealing with the duties and rights for every controller and pursuant to the Article 3(1) of extra-territoriality, it attempts to cover each and every aspect involving the transfers involving EU. Moreover, the imposing penalties of such extent also implies that EU is making constant efforts to eliminate any breach of data protection or privacy rights. Otherwise such restrictions on the transferring of personal data to third countries and such penalties wouldn't have been considered in the very first place. It shows that the measure so taken by the EU is legitimate to protect its fundamental interest.[43]

- **The Chapeau**

The ever-so-demanding second leg of the test however, is not so simple to prove. Here, the EU has to prove that such measures adopted by them are applied in a manner that is not discriminatory, arbitrable or unjustifiable. In such a case, the regime of the other third countries would be considered just similar to that when considering the adequacy requirements. However, when the adequacy question is considered it may turn to the fact that EU has a regime which is too strict to comply with and the fact there have been no alternate measures taken by the EU could lead to the conclusion that the said measures may not be justified by Article XIV. [44] Considering the strictness of the regime, there is a risk that the same measure could be challenged being in violation with GATS, MFN and Market access application. And when in force and it would then be difficult to justify the applicability of the same.

Having analysed the potentially trade restrictive measures and its impact on non-trade concerns. The next chapter finally attempts conclude by summarising this interesting debate.

---

[42] Yi-Hsuan Chen, 'The EU Data Protection Law Reform: Challenges for Service Trade Liberalization and Possible Approaches for Harmonizing Privacy Standards into the Context of GATS' (2015) 19 Spanish Yearbook of International Law. p219.

[43] The justification has been made keeping in mind the the DPD provisions as well and the idea has been borrowed from this article. Perez Asinari, "The WTO and The Protection of Personal Data. Do EU Measures Fall Within GATS Exception? Which Future for Data Protection Within the WTO e-commerce Context?" (BILETA. 2003) <http://www.bileta.ac.uk/content/files/conference%20papers/2003/The%20WTO%20and%20the%20Protection%20of%20Personal%20Data.%20Do%20EU%20Measures%20Fall%20within%20GATS%20Exception.pdf> accessed 11 August 2017.

[44] Mannheimer Swartling, 'Data Flows- Allowing Free Trade Agreements to Strengthen The GDPR' (2016) <http://www.mannheimerswartling.se/globalassetes/publikationer/data-flows.pdf> accessed 29 July 2017.