DINASTI RESEARCH
JLPH: Journal of Law, Politic and Humanities
E-ISSN: 2962-2816
P-ISSN: 2747-1985
https://dinastires.org/JLPH dinasti.info@gmail.com +62 811 7404 455
DOI: https://doi.org/10.38035/jlph.v6i5

Normative Review of EU Unilateral Data Flow Regulation and Non-Discrimination

Annisa Fitria[1*], Rita Alfiana[2]
[1]Faculty of Law, Universitas Esa Unggul, Jakarta, Indonesia
[2]Faculty of Law, Universitas Esa Unggul, Jakarta, Indonesia

[*]Corresponding author : annisa.fitria@esaunggul.ac.id

Abstract: The rapid expansion of the digital economy has intensified regulatory tensions surrounding cross-border data flows. The European Union's unilateral measures—particularly the General Data Protection Regulation (GDPR) and the adequacy decision mechanism—have reshaped global data governance. While intended to safeguard personal data, these measures raise concerns regarding their compatibility with the principle of non-discrimination under the WTO/GATS framework and their broader implications for international digital trade. This study employs a normative legal research approach, analyzing primary legal sources including the GDPR, WTO/GATS provisions, adequacy decisions, and relevant jurisprudence of the Court of Justice of the European Union. It also incorporates comparative policy analysis and doctrinal interpretation to evaluate the trade-related effects of the EU's unilateral regulatory actions. The research aims to assess whether the EU's unilateral regulation of cross-border data transfers constitutes a legitimate exercise of regulatory sovereignty or functions as a disguised restriction on trade. It further seeks to examine the extent to which such measures align with the non-discrimination principle in international digital trade law. The findings indicate that although the GDPR's extraterritorial scope enhances global data protection standards, its compliance requirements impose disproportionate burdens—particularly on developing countries—potentially amounting to non-tariff barriers. Selective adequacy decisions risk undermining multilateralism, contributing to regulatory fragmentation, and widening the global digital divide. This study contributes a normative trade-law perspective to the discourse on EU data governance, critically linking data protection regulation with WTO non-discrimination principles and highlighting the need for more inclusive, transparent, and multilateral digital governance reforms.

Keywords: Cross-Border Data Flows; GDPR; Adequacy Decisions; Non-Discrimination Principle; International Digital Trade.

INTRODUCTION

In the global digital era, cross-border data flows have become the main backbone of international trade, innovation, and digital services. However, the increasing unilateral regulation by countries, especially the European Union (EU), on cross-border data flows is creating tension between national sovereignty and multilateral international legal norms. The European Union, thru the General Data Protection Regulation (GDPR), has set strict standards for the transfer of personal data outside its territory. This rule is not only enforced domestically, but also has extraterritorial reach, affecting third countries that wish to process the data of EU citizens. One of the key mechanisms in this policy is the adequacy decision, which is an assessment of whether a country has a level of data protection considered "adequate" according to EU standards. Countries that fail to meet these standards will face significant obstacles in transferring data to and from the EU.(W. Gregory Voss, 2020)

Although this regulation is claimed to aim at protecting privacy rights as a fundamental human right, many parties criticize that this approach also serves as an instrument of digital protectionism and global regulatory dominance. The implications of this approach have raised concerns about the principle of non-discrimination in international digital trade, particularly for developing countries that do not have similar regulatory capacity. In this context, a number of studies indicate that the GDPR policy indirectly creates new trade barriers and adds a significant compliance burden for EU partner countries, especially those that do not yet have GDPR-level data protection standards. Additionally, the EU's unilateral approach could disrupt the spirit of global cooperation needed to establish fair and transparent international data governance.(Huang, 2023) This imbalance raises critical questions about how international law can respond to the trend of digital unilateralism and uphold fundamental principles such as justice, transparency, and equal access in the global digital economy.(Lee et al., 2019) This imbalance raises critical questions about how international law can respond to the trend of digital unilateralism and uphold fundamental principles such as justice, transparency, and equal access in the global digital economy.

METHOD

This study employs a normative legal research method with a doctrinal approach to examine the legal implications of the European Union's unilateral regulation of cross-border data flows, particularly through the General Data Protection Regulation (GDPR) and the adequacy decision mechanism, in relation to the principle of non-discrimination under international digital trade law. The research adopts several approaches. First, the statutory approach, which analyzes relevant legal instruments including the General Data Protection Regulation (GDPR), the General Agreement on Trade in Services (GATS), particularly Articles II, XIV, and XVII, and other international legal frameworks related to cross-border data governance. Second, the conceptual approach, which examines legal doctrines and theoretical concepts concerning regulatory sovereignty, digital protectionism, extraterritorial jurisdiction, non-discrimination principles, and digital trade governance. Third, the comparative approach, which compares the European Union's data governance framework with broader international trade norms and selected practices in global digital regulation. The legal materials used in this research consist of primary, secondary, and tertiary legal materials. Primary legal materials include international agreements, EU regulations, adequacy decisions, and relevant jurisprudence. Secondary legal materials comprise academic journal articles, books, legal commentaries, and policy reports discussing GDPR, international trade law, and digital governance. Tertiary legal materials include legal dictionaries and supporting reference sources.

The collection of legal materials is conducted through library research by systematically reviewing legal documents and scholarly literature. The analysis technique applies qualitative legal analysis using deductive reasoning, interpreting legal norms and assessing whether the European Union's unilateral regulation of cross-border data transfers constitutes a legitimate exercise of regulatory authority or potentially functions as a disguised restriction on trade under the WTO/GATS framework. This study further evaluates whether the EU's adequacy mechanism complies with the principle of non-discrimination and contributes to coherent and inclusive international digital governance.

RESULTS AND DISCUSSION

The European Union's Unilateral Regulation Of Cross-Border Data Flows Through Data Protection Policies, Particularly The Adequacy Decision Mechanism.

The Principle of Non-Discrimination in International Digital Trade. The principle of non-discrimination is one of the main pillars of international trade law, aiming to create equal treatment among countries in trade activities. In the context of international digital trade, this principle is becoming increasingly important because data has become a strategic commodity, equivalent to goods and services in the digital economy era. In the WTO system, the principle of non-discrimination is reflected thru two main provisions:

1. Most-Favoured-Nation (MFN) Treatment (Article II GATS): requires WTO members not to treat any particular country more favorably than others, except where justified exceptions exist.
2. National Treatment (Article XVII GATS): requires member states not to treat foreign service providers less favorably than domestic service providers.

These two principles are complementary, ensuring that no country or business operator is unfairly disadvantaged in international trade.(Kortukova & Nevara, 2023) In the context of digital services and cross-border data flows, this principle aims to ensure that countries do not implement policies that hinder or discriminate against foreign digital businesses' access to the market. The digital economy relies on system interoperability and cross-border data flows. Therefore, discrimination in the form of barriers to data access, imposing heavy legal compliance burdens on certain countries, or provisions that apply only to specific jurisdictions can be considered a violation of the spirit of non-discrimination. In practice, various countries impose restrictions on data flows thru mechanisms such as:

1. Data localization requirements;
2. Adequacy decision;
3. Administrative approval for data transfer;
4. Unequal privacy standards.

In GATS Article XIV(c)(ii), there is an exception that allows countries to impose restrictions for the protection of personal data privacy. However, this exception is not absolute and must meet three main conditions:

1. Policies must be implemented to protect a legitimate public policy goal;
2. It must be "necessary" to achieve that goal;
3. It must not constitute arbitrary or unjustifiable discrimination or a disguised restriction on trade.

Although GATS Article XIV(c)(ii) provides an exception for regulations that protect personal data, such policies must meet a three-part test: First, a legitimate objective; Second, necessary; and Third, not a disguised barrier to trade. Based on WTO practice, such as in the US – Gambling and Korea – Beef cases, the "necessity test" principle requires evaluation of less restrictive but still effective policy alternatives.(TRADE & ORGANIZATION, 2004) If GDPR can be achieved thru other, less restrictive approaches, the adequacy mechanism may be considered trade-unconstitutional. This is important considering GDPR has a high extraterritorial reach.

The European Union (EU) implements very strict data protection policies thru the General Data Protection Regulation (GDPR). One form of unilateral EU action is the implementation of the "adequacy decision" mechanism, where the European Commission can assess whether a third country has a level of personal data protection equivalent to EU standards. If a country is deemed "adequate," data transfers from the EU to that country can be made without additional requirements. Otherwise, the transfer can only be made with additional protection such as standard contractual clauses or binding corporate rules.(Huang, 2023)

Standard contractual clauses (SCCs) are standard contract clauses that have been pre-approved by the European Commission as an "appropriate safeguard" to allow the transfer of personal data outside the EEA (European Economic Area) in accordance with Article 46(2)(c) GDPR. The main characteristics of this Sccs are:

1. Designed for various transfer scenarios: controller-to-controller (C2C), controller-to-processor (C2P), processor-to-processor (P2P), processor-to-controller (P2C);
2. Allows more than two parties to adopt this clause, permits sub-processors, and grants "third-party beneficiary rights" to individuals;
3. A "transfer impact assessment" is mandatory: it assesses risks, checks local regulations, and takes additional measures if necessary;
4. Loading rules related to public authority access, such as notification obligations and legal challenges to unauthorized data requests.

Meanwhile, Binding Corporate Rules (BCRs) are legally binding internal policies for data transfers between entities within a multinational corporate group, as stipulated in Article 47 of the GDPR.(commission.europa.eu/law, n.d.) In the approval process for data exchange, the following are required:

1. Submitted to the data protection authority (DPA);
2. Involving the consistency mechanism and opinions from the European Data Protection Board (EDPB) before final approval.

So both SCC mechanisms are fast and practical mechanisms for cross-border data transfer, with strong contractual protection. Suitable for various scenarios such as controller-to-processor and vise versa. BCRs are a more strategic and comprehensive option for multinational companies seeking to ensure consistent data protection across global entities, but they require regulatory approval and investment in governance. Some academics, including Saluste, argue that policies like the EU's adequacy decision do not always meet the "least trade-restrictive" test, as they place a disproportionate burden on countries that do not have the same regulatory capacity as the EU.(Saluste, 2025)

Criticisms of the application of the non-discrimination principle in digital trade practices include:

1. The exceptions are political and biased: EU strategic partner countries find it easier to obtain adequacy status than Global South countries, even tho their data protection systems are not always better. (Sun, 2023)
2. Inconsistent and non-transparent standards: There are no globally agreed-upon multilateral criteria for what constitutes "adequate" data protection.(Yi-Hsuan Chen, 2015)
3. Lack of appeal mechanisms and participation from developing countries: The adequacy process is conducted unilaterally without an open forum for equal negotiation.(Yakovleva & Irion, 2020)

This shows that the principle of non-discrimination in the digital context is vulnerable to being overlooked when national or regional regulations have extraterritorial scope without considering the impact on other countries. The General Data Protection Regulation (GDPR) is applied extraterritorially, governing the processing of data of EU citizens by entities outside the EU region. One of its main tools is the adequacy decision mechanism, which allows data to be transferred only to countries considered to have an "adequate" level of data protection according to EU standards.

Although the purpose of GDPR is to protect privacy rights as a fundamental right, the implementation of these mechanisms is often criticized as a form of digital protectionism. Non-EU countries that do not obtain adequacy status must implement complex technical and legal instruments, such as Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs), which require significant resources and impact developing countries' participation in global digital trade.(W. Gregory Voss, 2020)

The European Union's (EU) "adequacy decision" mechanism is a process by which the European Commission assesses whether a third country or international organization provides personal data protection equivalent to EU standards. This mechanism is crucial for regulating cross-border data transfers and safeguarding fundamental rights to data protection. Basic Adequacy Decision Principle: Principle of Equivalent Protection The transfer of personal data to a third country is only permitted if that country guaranties a level of data protection that is "equivalent" or "essentially equivalent" to that applicable in the EU.(Araújo, 2015)

This principle aims to ensure that the privacy rights of EU citizens remain protected even when data is processed outside the EU. Then, the basic principle of the adequacy decision includes a comprehensive assessment: the European Commission conducts a thorough evaluation of the legal system, law enforcement, and data protection practices in the destination country. This assessment covers legal, institutional, and the effectiveness of individual rights protection.(Araújo, 2015)

In the context of international trade law, particularly under the General Agreement on Trade in Services (GATS), the principle of non-discrimination requires that countries must not treat trading partners differently unless there are justifiable objective reasons. Some studies assess that the EU's adequacy decision contradicts this principle because it results in unequal treatment of partner countries whose data protection systems are not identical to the EU's. Saluste demonstrates that although GATS Article XIV allows for exceptions for privacy protection, GDPR policies must still be proportionate thru a necessity test and not used as a disguised barrier to trade.(Saluste, 2025) In practice, the selective application to certain countries (e.g., recognition of Japan but not India) demonstrates the potential for discrimination not always based on objective standards.(Yi-Hsuan Chen, 2015)

The EU is effectively exporting its data standards to third countries thru a law by export approach. Countries like Japan, South Korea, and Israel are striving to adopt EU standards to achieve adequacy status, while Global South nations face structural barriers in making legal adjustments.(Kato, 2020) According to Huang, the adequacy mechanism can be considered a new form of non-tariff barrier that contradicts the spirit of free data trade.(Huang, 2023) This creates an asymmetrical global structure where the EU sets the direction for global standards, without any multilateral agreement. Research by Yakovleva and Irion confirms that the dominance of GDPR creates tension between the principles of digital sovereignty and international trade commitments.(Yakovleva & Irion, 2020) Within the GATS framework, privacy policies can be justified, but they still require proof that they are no more restrictive than necessary (least trade-restrictive). In some cases, the GDPR is considered to exceed those limits.

Developing countries tend to be victims of this imbalance. They not only face administrative and technical burdens to comply with GDPR but also experience restrictions in accessing the European digital market. Voss noted that without technical assistance and international harmonization, the EU's approach would widen the global digital divide.(W. Gregory Voss, 2020) The implementation of GDPR and the adequacy decision mechanism by the European Union has significant consequences for developing countries, both in terms of the digital economy, equal market access, and national regulatory capacity. This unilateral approach not only exacerbates global asymmetry in data governance but also potentially creates de facto non-tariff barriers (NTBs) to developing countries' participation in global data flows.

Most developing countries do not yet have adequate legal and institutional infrastructure to meet the strict data protection standards required by the GDPR. To achieve adequacy status, a country must build a data protection system equivalent to European standards, including an independent supervisory authority, enforcement mechanisms, strong individual rights, and a risk assessment system. For countries with limited resources, this becomes a very large and disproportionate burden. According to Lee et al., the cost of implementing regulations compatible with GDPR can hinder the competitiveness of small and medium-sized enterprises (SMEs) in developing countries, considering the need to hire data protection experts, invest in information security technology, and comply with periodic legal audits.(Lee et al., 2019) As a result, many businesses in developing countries choose not to engage in digital trade with Europe due to the high compliance costs and legal risks involved.

In practice, adequacy status is more easily granted to developed countries or the EU's political strategic partners (such as Japan, South Korea, and Canada), compared to Global South countries, which may have developing legal systems but are not yet "formally recognized." This creates unequal treatment that is de facto discriminatory. Sun shows that the European Commission's adequacy evaluation process is non-transparent and unilateral, with no objective and uniform standards that partner countries can use to determine the requirements they must meet.(Sun, 2023) This uncertainty strengthens the EU's bargaining position as the sole regulator of global data standards and disadvantages developing countries that lack equivalent geopolitical influence.

For developing countries that rely on digital service exports, such as customer service, data processing, and software development, bans or obstacles to data transfer from Europe could disrupt global digital supply chains. Outsourcing and BPO (business process outsourcing) activities in countries like India, the Philippines, and Kenya are highly dependent on the smooth cross-border data transfer. If those countries do not obtain adequacy status, data flows will be diverted to other EU-approved jurisdictions, leading to direct economic losses and long-term digital marginalization.(Huang, 2023)

The EU's approach creates a "regulatory imperialism" effect, where powerful countries export their norms without considering the local capacity or needs of other countries. This reinforces normative fragmentation in international law, where only the standards of developed countries are used as a reference. As noted by Yakovleva and Irion, unilateral regulations like GDPR disregard the principles of inclusivity and fairness in global decision-making. Developing countries become "passive followers" of standards they did not formulate but are required to adhere to.(Yakovleva & Irion, 2020)

Unlike the principle of common but differentiated responsibilities (CBDR) in international environmental law, which recognizes differences in capacity among countries, there is no adequate technical assistance mechanism in the global data protection regime for developing countries to adapt. The European Union rarely provides financial or technical support in the data harmonization process, leaving developing countries to adapt on their own, even tho they are normatively impacted by EU policies. This contradicts the principles in Agenda 2030 and the Sustainable Development Goals (SDGs), particularly the targets for inclusivity and reducing global inequality.

Implications of the European Union's unilateral actions on the application of the non-discrimination principle in international digital trade according to the global trade legal framework (e.g., WTO/GATS)

The European Union's (EU) unilateral actions in regulating cross-border data flows, particularly thru the General Data Protection Regulation (GDPR) and adequacy decisions, have created a new dynamic in international law. On the one hand, the action is based on the state's sovereignty in protecting the personal data of its citizens. However, on the other hand, such unilateral policies create tension against the principle of multilateralism, particularly in the context of international trade agreements and global digital governance. Yakovleva and Irion state that the EU has become the dominant actor in shaping global privacy standards, often without coordination with multilateral bodies such as the WTO or OECD. This is referred to as a form of "unilateral rule-export" that threatens equality in the process of international norm-making.(Yakovleva & Irion, 2020)

GDPR applies not only to entities within the EU, but also to companies outside the EU that process the data of EU citizens. This reflects the principle of regulatory extraterritoriality, which is often controversial in international law. This principle conflicts with the sovereignty of other countries, especially when the EU "imposes" its privacy standards on jurisdictions not directly involved in the rule-making process. According to Chen, the extraterritorial application of GDPR without multilateral agreements creates "normative unilateralism," which is the tendency of one country or region to impose its domestic laws on the global stage without a consensus mechanism.(Yi-Hsuan Chen, 2015)

The principle of non-discrimination is one of the fundamental principles in international law, both in the field of human rights and in international economic and trade law. This principle demands that every individual or entity be treated equally without discrimination based on race, gender, religion, nationality, or other objectively irrelevant characteristics.(KOBZAR-FROLOVA & Frolov, 2025) In the context of international law, this principle serves as a legal guaranty that all people can enjoy their rights and freedoms without exception.(Mekhaneg, 2023)

Implications for the Principle of Non-Discrimination:

1) Potential Non-Tariff Barriers.
   The EU's policy restricting the transfer of personal data only to countries with a level of data protection deemed "adequate" can be seen as a non-tariff barrier in digital trade. Countries that do not obtain adequacy status face restrictions on access to the EU's digital market, potentially violating the principle of non-discrimination in GATS and the WTO, where member states are supposed to provide equal treatment to all trading partners.(Yakovleva & Irion, 2020)
2) Justification Based on Fundamental Rights.
   The EU justifies this restriction on the grounds of protecting fundamental rights to privacy and personal data, which are recognized in EU law. Within the WTO/GATS framework, such restrictions can be justified if they meet the "necessity test"—that is, the restriction must be necessary to protect legitimate public interests, such as privacy, and no more restrictive than necessary. However, some analyzes suggest that the EU's restrictions may exceed what is permitted under WTO commitments, creating tension between data protection and the principle of non-discrimination.(Yakovleva & Irion, 2020)
3) Regulatory Fragmentation and Extraterritorial Effects.
   The EU's unilateral actions also promote global regulatory fragmentation, as other countries are compelled to adjust their standards to access the EU market. This creates regulatory pressure (the California Effect) and can trigger other countries to implement similar policies, ultimately complicating cross-border digital trade and challenging the principle of non-discrimination.(Bendiek & Römer, 2019)
4) Opportunities and Challenges for Digital Trade.
   While this policy could boost consumer confidence and demand for foreign digital products in the EU, high compliance costs and legal uncertainty could pose barriers for businesses from countries that do not obtain adequacy status. This could potentially hinder fair competition in international digital trade.(Li et al., 2025)
5) Opportunities and Challenges for Digital Trade.
   While this policy could boost consumer confidence and demand for foreign digital products in the EU, high compliance costs and legal uncertainty could pose barriers for businesses from countries that do not obtain adequacy status. This could potentially hinder fair

competition in international digital trade.(Li et al., 2025)

Fragmentation of international law refers to the phenomenon where various legal systems, regimes, or international treaties develop separately, often with potentially overlapping, conflicting, or mutually negating principles, procedures, or objectives. This term has become increasingly relevant in the last decade as global issues—including human rights, trade, the environment, and digital data—are managed by various international forums that are not always systematically coordinated. The International Law Commission (ILC) in its annual report cited fragmentation as the main challenge of the 21st century in maintaining the coherence and integrity of international law. In the issue of cross-border data flows, fragmentation arises due to the absence of a single, universally agreed-upon international legal framework. As a result, several regimes and actors have taken their own approaches, creating a fragmented global regulatory landscape:

1. The European Union with a strict privacy protection approach thru the GDPR and adequacy decisions.
2. The United States with a sectoral approach based on the principles of accountability and commercial interests.
3. China with a cyber-sovereignty approach and strict state control over outgoing data flows.
4. The WTO, thru GATS and CPTPP, is attempting to incorporate data issues into trade agreements.

Because there is no clear multilateral agreement on data protection standards or data transfer rules, fragmentation occurs both substantively (different content of the rules) and institutionally (different forums for norm creation). Forms of Fragmentation:

1. Substantive Fragmentation This occurs when the legal principles of different regimes conflict in content. For example:
   a. GDPR makes data protection rights a fundamental human right, while the WTO and GATS prioritize non-discrimination and trade liberalization.
   b. The OECD regime emphasizes data interoperability, whereas the EU approach prioritizes evaluative and unilateral adequacy.
2. Institutional Fragmentation This occurs when no single international body exclusively regulates data issues. As a result, countries can "choose" the most advantageous forum or rules (forum shopping), leading to overlapping authority between institutions such as the WTO, ITU, OECD, UNCTAD, and regional courts like the CJEU.
3. Procedural Fragmentation Dispute resolution mechanisms differ across regimes. In the WTO, there is a binding and formal dispute resolution process, while in data issues, there is no effective dispute resolution forum for cross-jurisdictional disputes related to the GDPR.

Impact of Fragmentation in International Law

1. Legal incoherence: States and companies struggle to navigate the diverse and even contradictory regulatory landscape.
2. Legal uncertainty: Without uniform international rules, countries issue their own regulations, increasing tensions.
3. Embrace multilateralism: Large countries like the EU can impose rules unilaterally, making global harmonization efforts difficult.
4. Global access gap: Developing countries are the most affected because they lack the capacity to meet all standards simultaneously.

For example, the incompatibility between GDPR and the US approach to data privacy led to the collapse of the Privacy Shield Agreement, leaving multinational companies in a state of regulatory uncertainty. This case demonstrates how fragmentation can have a direct impact on legal stability and cross-border trade relations. The EU's unilateral actions strengthen the fragmentation of international law in two aspects:

1. Legal substance: Countries must choose between following EU, US, China, or other regional systems, thus weakening efforts toward global interoperability.
2. International institutions: There is no established legal forum for resolving disputes related to digital data standards. The WTO does not yet have sufficient mechanisms to comprehensively address data privacy issues.

Saluste emphasized that the EU adequacy decision could potentially conflict with WTO member states' commitments under GATS, especially if used as a reason to restrict data transfers without proportionality and transparency testing. The most obvious implication of this unilateralism is felt by developing countries. These countries were forced to adjust their domestic regulations to comply with GDPR if they wanted to remain participants in the global digital economy. However, they did not have an equal opportunity to participate in the formulation of these rules.

Voss mentions that this practice creates "regulatory dependency," where Global South countries become objects of norms, not subjects creating norms. This contradicts the principle of equality in international law. The EU's digital unilateralism poses a crisis of legitimacy for international law, as it sidelines the deliberative multilateral mechanisms commonly used to establish global norms.(W. Gregory Voss, 2020) When international norms are formed without fair global representation, their legitimacy and enforceability can be questioned. Kwet refers to this phenomenon as part of "digital colonialism," where technological and legal power is used to subjugate the jurisdictions of other countries. In this context, international law becomes an arena of struggle between dominant norms and equal global participation.

The European Union's unilateral actions in digital data governance contribute to serious tensions in international law. On one hand, this action reflects the state's sovereign right to protect privacy. However, its extraterritorial application, without global consensus, has weakened the principle of multilateralism, strengthened the fragmentation of international law, and created structural inequalities, particularly for developing countries. Digital governance reform based on equality, global representation, and the rule of international law is needed to prevent unilateral dominance in the digital space, which is supposed to be inclusive and fair. Why is Digital Governance Reform Needed? Digital governance is currently dominated by a few global actors, particularly the European Union, the United States, and China, each of which implements legal and technological approaches based on its domestic interests. This imbalance has created an asymmetrical global digital power structure, where:

1. Developed countries set data privacy and security standards.
2. Developing countries are forced to adopt regulations without being involved in their creation (regulatory dependency).
3. There is no equal multilateral forum to formulate globally binding digital legal norms.

As a result, there is unilateral dominance in the digital space, which gives rise to protectionism, non-tariff barriers in data trade, and unequal access to digital technology. In international law, the principle of sovereign equality of states is a fundamental foundation. However, in the practice of digital governance, this principle is often overlooked because:

1. Developing countries lack the technical capacity and resources to participate in the development of digital norms;
2. Many Global South countries are merely recipients of policies, not active participants;
3. There is no effective global platform where countries can voice their interests equally.

Reform is needed to build inclusive digital governance, where developing countries can meaningfully participate in setting global standards, including thru South-South cooperation and engagement in forums like the WTO, ITU, or UNCTAD. Public international law, particularly thru instruments like GATS (WTO) and ICCPR, adheres to the principles of multilateralism, legal certainty, and dispute resolution mechanisms. However, currently:

1. The European Union, thru the GDPR and adequacy decisions, is implementing laws extraterritorially, without an international consensus process;
2. The United States relies on a sectoral approach without a unified federal framework;
3. China implements a closed principle of cyber-sovereignty.

This phenomenon has weakened the authority of international law in digital issues. International law supremacy is needed so that all countries are subject to collective rules, not the dominant norms of one party. As stated by Yakovleva & Irion (2020), "consistency between national digital policies and multilateral trade commitments is crucial to prevent the emergence of international legal fragmentation.

CONCLUSION

The European Union's unilateral actions thru the General Data Protection Regulation (GDPR) and the adequacy decision mechanism have positioned the EU as the global standard-setter for personal data protection. This mechanism allows the EU to only permit data transfers to countries deemed to have an equivalent level of data protection, while other countries must meet additional requirements such as Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs). This policy strengthens the protection of personal data, but it also presents significant challenges, such as a high compliance burden, especially for small and medium-sized businesses, and widens the global regulatory gap due to a lack of international legal harmonization.

The implications for the principle of non-discrimination in international digital trade are quite significant. Countries that do not obtain adequacy status face additional barriers in accessing the EU's digital market, which can be considered non-tariff barriers and potentially violate the principle of non-discrimination within the framework of global trade law such as the WTO/GATS. This risks causing fragmentation of the global digital trade system and increasing cross-country compliance costs.

REFERENCE

Araújo, A. M. R. (2015). The Right to Data Protection and the Commissions' Adequacy Decision. *UNIO – EU Law Journal*, *1*, 77–93. https://doi.org/10.21814/unio.1.6

Bendiek, A., & Römer, M. (2019). Externalizing Europe: the global effects of European data protection. *Digital Policy, Regulation and Governance*, *21*(1), 32–43. https://doi.org/10.1108/DPRG-07-2018-0038

commission.europa.eu/law. (n.d.). *data-protection/international-dimension-data-protection/binding-corporate-rules-*. Commission.Europa.Eu/Law. commission.europa.eu/law

Huang, L. (2023). How the Data Rules of EU is Exported to the Outside of the Region: Take the EU 's General Data Protection as an example. *Journal of Education, Humanities and Social Sciences*, *24*, 399–404. https://doi.org/10.54097/nxw6ds83

Kato, T. (2020). Reflections on the GDPR Adequacy Assessment and Strategy of Japan: For the Enhancement of Transborder Data Flows. *Global Privacy Law Review*, *1*(Issue 3), 156–163. https://doi.org/10.54648/GPLR2020092

KOBZAR-FROLOVA, M., & Frolov, V. (2025). THE PROBLEM OF NON-DISCRIMINATION IN THE MODERN WORLD AND WAYS TO STRENGTHEN THE EFFECT OF THE NORMS OF INTERNATIONAL TREATIES. *VESTNIK ADVANCED TRAINING INSTITUTE OF THE MIA OF RUSSIA*, 23–29. https://doi.org/10.29039/2312-7937-2025-1-23-29

Kortukova, T., & Nevara, L. (2023). FEATURES OF THE PRINCIPLE OF NON-DISCRIMINATION IN INTERNATIONAL TRADE AND ECONOMIC LAW. *Legal Horizons*, *17*(2), 040–050. https://doi.org/10.54477/LH.25192353.2023.2.pp.040-050

Lee, K. Y., Cho, M. hee, Kang, J., & Kang, M. (2019). Welfare Effects of the EU GDPR and Data Localization Measures. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3407208

Li, Z., Lee, G., Raghu, T. S., & Shi, Z. (Michael). (2025). Impact of the General Data Protection Regulation on the Global Mobile App Market: Digital Trade Implications of Data Protection and Privacy Regulations. *Information Systems Research*, *36*(2), 669–689. https://doi.org/10.1287/isre.2022.0421

Mekhaneg, A. (2023). The Status of the Principle of Non-Discrimination under the International Human rights Law. *Journal of Law, Society and Authority*, *12*(2), 12–29. https://doi.org/10.52919/lsa.v12i2.192

Saluste, M. (2025). Cross-Border 'Data Adequacy' Frameworks under GATS Article VII: Aligning WTO Members' Rights to Protect Personal Data with Their International Commitments. *World Trade Review*, 1–27. https://doi.org/10.1017/S1474745625000047

Sun, L. (2023). Overview of Regulations on Cross Border Data Flow. *Academic Journal of Science and Technology*, *8*(1), 171–176. https://doi.org/10.54097/ajst.v8i1.14305

TRADE, W., & ORGANIZATION. (2004). *UNITED STATES – MEASURES AFFECTING THE CROSS-BORDER SUPPLY OF GAMBLING AND BETTING SERVICES*.

W. Gregory Voss. (2020). CROSS-BORDER DATA FLOWS, THE GDPR, AND DATA GOVERNANCE. *Washington International Law Journal Association*, *29*, 485. https://doi.org/https://doi.org/10.2139/ssrn.3435988

Yakovleva, S., & Irion, K. (2020). Toward Compatibility of the EU Trade Policy with the General Data Protection Regulation. *AJIL Unbound*, *114*, 10–14. https://doi.org/10.1017/aju.2019.81

Yi-Hsuan Chen. (2015). THE EU DATA PROTECTION LAW REFORM: CHALLENGES FOR SERVICE TRADE LIBERALIZATION AND POSSIBLE APPROACHES FOR HARMONIZING PRIVACY STANDARDS INTO THE CONTEXT OF GATS. *Spanish Yearbook of International Law*, *19*, 211–220. https://doi.org/10.17103/sybil.19.13