

DATA PROTECTION AND CROSS BORDER DISPUTES

AUTHOR – FARZILA, STUDENT AT TAMIL NADU DR AMBEDKAR LAW COLLEGE

BEST CITATION – FARZILA, DATA PROTECTION AND CROSS BORDER DISPUTES, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 6 (9) OF 2026, PG. 757-764, APIS – 3920 – 0001 & ISSN – 2583-2344.

ABSTRACT

The fast-paced developments in digital technology, cloud computing, artificial intelligence, and internet communication across the globe have resulted in greater flows of personal data internationally. Cross-border flows of data have contributed immensely to the processes of economic development, innovation, and international collaboration; however, the issue of cross-border personal data flow presents several legal problems as well. The disparities among national laws of data protection, the practices of government surveillance, cyber security threats, and jurisdictional issues have posed a number of cross-border controversies. The objective of this research paper is to study the issue of data protection law and the issues involved in regulating international data management. In this context, the research will look into the primary causes that lead to data protection issues at an international level. In addition, the paper will compare how Europe, the US, and India protect and regulate data management practices. Apart from this, the research will examine the role played by international organizations as well as the role of judicial decisions in the regulation of data protection. Moreover, some of the challenges related to data protection include non-uniformity in legislation, poor enforcement, and rapid technological development impacting privacy.

PART 1 – INTRODUCTION

1.1 Background of the Study

Personal data has become a highly valued resource due to the current digitalization era.¹⁴¹⁹ With advancements in technology, use of the Internet, cloud computing, artificial intelligence, and digital communication, personal information is now gathered, stored, analyzed, and sent abroad more easily than before.¹⁴²⁰ People tend to give their personal information through such channels as social media, e-commerce sites, banking apps, healthcare networks, and educational platforms online. Therefore, massive amounts of data transfer occur on a daily basis between different countries around the world.¹⁴²¹

As far as data transfer between states becomes increasingly common, privacy becomes a highly questionable issue.¹⁴²² Multinational firms and large tech companies work and operate in different countries at the same time.¹⁴²³ Thus, users' data can be sent from one country to another to perform any activity related to their operations. While cross-border data flows promote international relations and cooperation between countries, it poses challenges to privacy regulations.¹⁴²⁴

Cross-border data controversies have become quite frequent owing to issues such as cyber-attacks, unauthorized exchange of information, foreign surveillance techniques, and discrepancies between different jurisdictions.¹⁴²⁵ Since there is no standard legal regime governing international data exchange, this

¹⁴¹⁹ Daniel J. Solove & Paul M. Schwartz, *Information Privacy Law* 3–8 (7th ed. 2021).

¹⁴²⁰ Lee A. Bygrave, *Data Privacy Law: An International Perspective* 1–5 (2014).

¹⁴²¹ Organisation for Economic Co-operation and Development (OECD), *OECD Digital Economy Outlook 2020* 15–18 (2020).

¹⁴²² Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890).

¹⁴²³ Christopher Kuner, *Transborder Data Flows and Data Privacy Law* 12–19 (2013).

¹⁴²⁴ Paul M. Schwartz, *Global Data Privacy: The EU Way*, 94 N.Y.U. L. Rev. 771, 775–80 (2019).

¹⁴²⁵ Frank Pasquale, *The Black Box Society* 3–10 (2015).

poses challenges in the choice of appropriate law, enforcement of the decision, and safeguarding user interests.¹⁴²⁶ Hence, the regulation of international data has become a significant area for study in current times.

The purpose of this research is to study the problems involved in the protection of data as well as resolving any dispute that may arise in the realm of international data governance.

1.2 Research Questions

1. What are the major legal challenges involved in cross-border data protection disputes?
2. How do different countries regulate international data transfers and privacy protection?
3. What role do international organizations and legal frameworks play in international data governance?
4. Why is there a need for harmonized global standards for data protection?¹⁴²⁷

1.3 Research Objectives

1. To examine the concept and importance of data protection in the digital era.
2. To analyze the causes and challenges of cross-border data disputes.
3. To compare international data protection frameworks such as the GDPR, US privacy laws, and Indian data protection laws.¹⁴²⁸
4. To evaluate the effectiveness of international data governance mechanisms.
5. To suggest measures for improving international cooperation and dispute resolution in data protection matters.

1.4 Scope of the Study

The paper will be focusing on the challenges associated with data protection and cross-border legal disputes in the governance of data. Specifically, the flow of data across borders and the disputes that occur as a result of disparities between the privacy laws of the different nations will be the major point of interest. The analysis of this study will be focused on legal aspects associated with data governance, especially within the EU, the US, and India, among others.¹⁴²⁹

The limitations associated with this study include doctrinal/analytical research using legislation, international law, case laws, scholarly works, and policy papers. This research is not empirically driven. This research is also limited in that it deals with privacy, jurisdictional conflicts, cybersecurity issues, data localization, and international cooperation in data governance.¹⁴³⁰

PART 2

CONCEPT OF DATA PROTECTION AND INTERNATIONAL DATA GOVERNANCE

2.1 Meaning and Scope of Data Protection

Data Protection is defined as the implementation of laws and regulation which helps in protecting personal information from any kind of access, misuse, disclosure, modification, or destruction.¹⁴³¹ Personal data in the modern era includes names, addresses, telephone numbers, financial information, biometric information, health information, web surfing habits, and other personal identifiable information. The main aim behind the implementation of the law for data protection is to make sure that personal information is collected and processed in a fair, lawful, and safe manner.

Data Protection and Privacy are related to each other in the sense that the right to privacy is considered as a basic human right in most of the

¹⁴²⁶ Graham Greenleaf, Global Data Privacy Laws 2023: 168 National Laws & Many Bills, 181 Privacy Laws & Bus. Int'l Rep. 10 (2023).

¹⁴²⁷ OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Sept. 23, 1980.

¹⁴²⁸ General Data Protection Regulation, Regulation (EU) 2016/679, 2016 O.J. (L 119) 1.

¹⁴²⁹ Julia Hörnle et al., Data Protection, Privacy and Information Law 25–30 (2018).

¹⁴³⁰ Dan Jerker B. Svantesson, Solving the Internet Jurisdiction Puzzle 45–49 (2017).

¹⁴³¹ General Data Protection Regulation, Regulation (EU) 2016/679, art. 5, 2016 O.J. (L 119) 1.

legal jurisdictions of the world.¹⁴³² In particular, informational privacy is known to be the right of an individual who has to control his personal information. Due to the rapid development in digital communication, there has been an urgent need to protect personal information since personal information is regularly shared by individuals on social networking sites, banking channels, healthcare portals, and e-commerce websites.¹⁴³³

2.2 Evolution of Data Protection Laws

The idea of safeguarding personal information has been evolving with advances in technology.¹⁴³⁴ The issue of privacy first arose with the emergence of systems of record-keeping by governments and use of computers for data storage at the beginning of the twentieth century. At that time, the issue of privacy was associated only with illegal invasion of people's lives.

The first data protection legislation appeared in the 1970s and originated in Europe.¹⁴³⁵ Initially, it sought to regulate the automatic processing of personal information by both public bodies and private enterprises. Later, international organizations started to work out international guidelines to ensure proper data treatment and set minimal requirements for privacy protection.

A landmark for international privacy protection regulations is the introduction of the General Data Protection Regulation (GDPR).¹⁴³⁶ It was adopted in the European Union and imposes strict rules for organizations processing personal information. In addition, GDPR introduces many individual rights related to their personal information and regulates the issue of cross-border transfer of such data.

2.3 International Data Governance

By international data governance, one can mean the system of laws, policies, and institutional structures that govern the process of collecting, processing, storing, transferring, and protecting data internationally.¹⁴³⁷ In this regard, with the development of globalization processes where information is shared between countries worldwide via interconnected networks, good governance in relation to the issue of international data transfer has become crucial.

It should be noted that today, due to multinational companies' development, the international data transfer problem became topical. Companies may collect and process data in servers situated in different countries using cloud computing services.¹⁴³⁸ While the process brings some benefits, it also raises some issues related to differences in countries' privacy regulations.

PART 3

CROSS-BORDER DATA TRANSFERS AND EMERGING DISPUTES

3.1 Causes of Cross-Border Disputes

Data-related disputes occurring internationally can be described as any form of disagreements among persons, organizations, or government agencies about the collection, transmission, processing, and protection of people's data from one state to another.¹⁴³⁹ As technologies continue to advance, such disputes have been on the rise.

Jurisdictional conflicts are one source of international data disputes. Because data passes through several jurisdictions at once, it can become difficult to establish which law governs a dispute. Different legal systems could impose different requirements on a firm,

¹⁴³² Universal Declaration of Human Rights art. 12, G.A. Res. 217A (III), U.N. Doc. A/810 (Dec. 10, 1948).

¹⁴³³ Daniel J. Solove & Paul M. Schwartz, *Information Privacy Law* 15–20 (7th ed. 2021).

¹⁴³⁴ Lee A. Bygrave, *Data Privacy Law: An International Perspective* 56–60 (2014).

¹⁴³⁵ Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Jan. 28, 1981, E.T.S. No. 108.

¹⁴³⁶ General Data Protection Regulation, Regulation (EU) 2016/679, 2016 O.J. (L 119) 1.

¹⁴³⁷ Julia Hörnle et al., *Data Protection, Privacy and Information Law* 25–30 (2018).

¹⁴³⁸ Christopher Kuner, *Transborder Data Flows and Data Privacy Law* 12–19 (2013).

¹⁴³⁹ Christopher Wolf et al., *Managing Privacy Through Accountability* 14–17 (2010).

depending on the type of issue involved. The company will find it challenging to fulfill obligations under the different laws.

Another reason that leads to data conflicts is government surveillance. Certain countries' national security laws provide government officials with access to the data of users stored in technology firms. Such surveillance practices could infringe the right of privacy accorded in other states. There have been some international disputes because of mass surveillance practices and unauthorized access by government to private data.

Commercial exploitation of people's data without prior consent has also caused much concern.¹⁴⁴⁰ In order to target users with advertisements, technology firms collect huge volumes of personal data for profiling and behavioral analysis purposes.

3.2 Challenges in Resolving Cross-Border Disputes

The resolution of disputes concerning cross-border data exchange is quite complicated due to the lack of a unified international legal framework governing data exchanges at an international level. First of all, the problem lies with the conflict of laws. Every country has different rules concerning privacy, consent, retention of data, surveillance, and so forth. Thus, while a certain practice may be regarded as legal in one country, it may contradict to the protection of privacy in another country.

Moreover, it is difficult to establish jurisdiction over cross-border data exchanges and decide on which set of laws will govern the dispute.¹⁴⁴¹ Due to the fact that digital activities are conducted simultaneously in several countries, it is difficult for courts to determine whose jurisdiction they fall under.^a

Cross-border enforcement of judgments can be another challenge.¹⁴⁴² Even when a judicial body

or administrative agency delivers a ruling against a multinational company, enforcement of such judgment in another jurisdiction may necessitate international collaboration. There could be jurisdictions that would not accept a foreign decision when it is contrary to their domestic laws or interests.

The existence of no common international standards makes dispute settlement difficult as well. Though international agencies have come up with guidelines and principles related to privacy, there has not been a globally-binding international agreement on the regulation of cross-border flows of information.

PART 4

COMPARATIVE ANALYSIS OF INTERNATIONAL DATA PROTECTION FRAMEWORKS

4.1 European Union Approach

Indeed, the European Union boasts one of the most robust and well-structured frameworks for protecting personal data in the world.¹⁴⁴³ First, it should be noted that the European model of privacy and data protection is largely based on recognition of privacy and personal data protection as human rights. Undoubtedly, the GDPR (General Data Protection Regulation) is the most important legal tool for ensuring data protection in the European Union, which entered into force in 2018.¹⁴⁴⁴

It is worth highlighting that the GDPR applies to all entities collecting or processing personal data belonging to residents of the European Union irrespective of the location of such an entity. Thus, this regulation is characterized by its extra-territorial applicability that makes it widely recognized in international data protection regulations. Importantly, the GDPR sets out a number of strict requirements for data controllers and processors concerning transparency, lawfulness, obtaining consent, accountability, and security of personal data.

¹⁴⁴⁰ Shoshana Zuboff, *The Age of Surveillance Capitalism* 8–12 (2019).

¹⁴⁴¹ Andrew T. Kenyon & Megan Richardson, *New Dimensions in Privacy Law* 101–05 (2006).

¹⁴⁴² Christopher Kuner, *Transborder Data Flows and Data Privacy Law* 85–90 (2013).

¹⁴⁴³ Charter of Fundamental Rights of the European Union arts. 7–8, 2012 O.J. (C 326) 391.

¹⁴⁴⁴ General Data Protection Regulation, Regulation (EU) 2016/679, 2016 O.J. (L 119) 1.

The GDPR provides individuals with a number of rights related to personal data protection. For example, according to this document, individuals are entitled to access, rectify, delete, restrict processing, or obtain their personal data processed in electronic format.

4.2 United States Approach

The US adopts a completely different approach in regards to the protection of data. While the EU has established a complete legislation on data protection that is binding for all sectors, the US does not have such an overarching law.¹⁴⁴⁵ Rather, it takes a more sectorial and industry-based approach, whereby each type of personal data falls under different legislations.

Healthcare data, financial data, consumer protection regulations and children's online privacy are examples of areas covered by sector-based legislation in the US.¹⁴⁴⁶ The American model of data regulation provides greater flexibility, thus fostering innovation and development in industries. Overall, this approach stresses economic growth, freedom of information flows and self-regulation of businesses.

On the other hand, the American model of data protection received criticism due to the problem of government surveillance and lack of adequate privacy safeguards. The presence of national security laws providing the intelligence community with access to personal information was seen as problematic in terms of harmonization with the GDPR.

4.3 Indian Approach

Digital revolution was observed in India due to greater internet accessibility, increase in the use of smartphones, internet banking, ecommerce expansion, and digitization efforts from the side of governmental bodies. With the development of digital services, there have been growing

worries about ensuring personal data protection and privacy.

The recognition of privacy as a basic right by the Supreme Court of India in the landmark case of Justice K. S. Puttaswamy v. Union of India became the important event in the field of Indian privacy law.¹⁴⁴⁷ It is indicated that informational privacy is a crucial aspect of individual liberty and dignity according to the Indian Constitution.

Thereafter, India enacted the Digital Personal Data Protection Act in order to regulate the personal data processing and ensure some obligations for companies working with personal data.¹⁴⁴⁸ The aim of the legislation is to regulate the lawful data processing, consent provisions, personal data security, and some other aspects.

India aims at ensuring privacy protection as well as economic development and innovations. Thus, the law emphasizes the importance of cross-border data transfer for international economic relations and digital development while considering some issues related to national security.

4.4 Comparative Evaluation

Legal philosophies and priorities in terms of privacy and cross-border data governance in the EU, US, and Indian data protection schemes differ.

Firstly, the EU is based on the principles of a rights-centric regime, where privacy is viewed as one of the fundamental human rights. Such approach imposes strict regulations on corporations and offers a high level of individual privacy protection.

On the other hand, the US relies on a more market-oriented sectorial regime, which is less strict compared to that of the European Union, and allows for greater freedom of innovations and economic development. Although the latter contributes to technological advancement,

¹⁴⁴⁵ Daniel J. Solove & Woodrow Hartzog, The FTC and the New Common Law of Privacy, 114 Colum. L. Rev. 583, 585–90 (2014).

¹⁴⁴⁶ Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936.

¹⁴⁴⁷ Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).

¹⁴⁴⁸ Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).

some critics argue that it has led to fragmented regulations and low levels of privacy protection.

India, finally, adopts a developing hybrid approach with regards to privacy regulation. Being an emerging digital economy, India finds itself facing several challenges associated with capacity to regulate the data protection sector and to balance between national security interests, economic development, and privacy protection.

Such differences in approach may cause many problems in the sphere of cross-border data transfer and international dispute resolution. Corporations will have to deal with multiple regulatory regimes at once, which increases legal complications.

PART 5

ROLE OF INTERNATIONAL ORGANIZATIONS AND JUDICIAL BODIES

5.1 Role of International Organizations

International bodies have played a crucial role in formulating principles, rules and frameworks for data protection and international data governance. Given that digital data crosses national boundaries without any geographical restrictions, there is no one country which can regulate global data flow on its own. Thus, international collaboration has become essential to protect privacy rights and settle disputes related to cross-border data.

Privacy has been recognized as an important human right by the United Nations in the digital age.¹⁴⁴⁹ The United Nations has highlighted through resolutions and reports the importance of safeguarding privacy and raised alarms about unauthorized surveillance, use of personal data and threats from cyber attacks faced by individuals worldwide. United Nations has urged countries to establish laws that provide transparency and accountability in handling personal data.

In a similar way, the Organization for Economic Co-operation and Development has formulated guidelines that deal with privacy and the protection of personal data and their transborder flow. The Organization has established various important principles including limitation of purposes,

data quality, security measures, openness and individual participation. Despite the fact that these principles are not legally binding, they have had great influence on domestic laws and international practices.

5.2 Important Case Laws

Several landmark judicial decisions have significantly influenced international data protection law and cross-border data governance.

One such notable case includes Schrems II, a ruling made by the Court of Justice of the European Union.¹⁴⁵⁰ The case involved a question on whether the transfer of personal data from the European Union to the United States was legal in light of the Privacy Shield agreement. The ruling overturned the agreement citing that US surveillance laws lacked adequate measures to protect the privacy of citizens.¹⁴⁵¹ This ruling had enormous effects on the multinational corporations who had been making use of such data transfers.

The two rulings showed the significance of adequate protection measures for the protection of personal data in international data transfers. They also indicated that conflicts in the implementation of privacy standards could arise through international litigation procedures. In the Indian context, the significant ruling was Justice K. S. Puttaswamy v. Union of India where the Supreme Court of India ruled that the right to privacy was a fundamental right guaranteed by the Constitution of India.¹⁴⁵² In this ruling of this case, the court ruled that informational privacy was a crucial part of personal liberty and dignity.

¹⁴⁴⁹ G.A. Res. 68/167, Right to Privacy in the Digital Age (Dec. 18, 2013).

¹⁴⁵⁰ Schrems v. Data Prot. Comm'r (Schrems II), Case C-311/18, ECLI:EU:C:2020:559.

¹⁴⁵¹ Commission Implementing Decision 2016/1250, 2016 O.J. (L 207) 1.

¹⁴⁵² Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).

PART 6

CHALLENGES IN INTERNATIONAL DATA GOVERNANCE

The management of international data involves multiple difficulties in terms of legal, technical, political, and economic factors as the digital transformation is taking place rapidly. Even though significant progress has been made concerning the establishment of data protection laws within recent years, the absence of an all-encompassing regulatory system on the global level results in a high degree of ambiguity in dealing with the issue of international data flows.

Firstly, there lacks an international law governing the regulation of personal data protection. Every country has its own legal approach to privacy, consent, surveillance, and the processing of personal information. To put it differently, while the EU applies stringent privacy regulations in accordance with the GDPR, the United States operates on the principle of sectoral approaches.

The issue of technological evolution makes things more complex with regard to international data governance¹⁴⁵³. Technologies such as artificial intelligence, big data analysis, machine learning, blockchain technology, and cloud computing process enormous amounts of personal data within a record time frame. At the same time, it is quite challenging to maintain transparency and accountability and obtain informed consent as technologies tend to be cross-jurisdictional.

Another critical issue that poses challenges for international data protection includes cybersecurity risks and data leaks.¹⁴⁵⁴ As cyberattacks are increasingly carried out against international businesses, banks, health organizations, and governmental authorities, they inevitably reveal private data of millions of citizens all around the globe. Given the fact that

most cybercrimes involve jurisdictions located abroad, it becomes extremely hard to investigate and enforce laws regarding cybercrimes.

The regulation of multinational technology companies presents another area of complexity.¹⁴⁵⁵ Large technology firms have vast economic strength and can operate within many jurisdictions. Regulatory agencies in different nations may find it difficult to enforce compliance with local privacy laws since the corporations will likely store their data and conduct their business activities in other jurisdictions as well. Further, the corporations could use the difference in regulations to lessen their regulatory burden.

Thus, international data governance should rely on global cooperation, legal harmonization, enforcement, and adaptation to technological advancements. Unless there are collective international approaches to tackling such issues, the task will continue to present challenges in the modern digital age.

PART 7

SUGGESTIONS AND RECOMMENDATIONS

With growing digitization and transfer of data across borders, there is an evident necessity of having better international data governance mechanisms to meet new challenges. Several recommendations concerning the improvement of legislation in the sphere and cooperation between the parties can be offered to overcome existing problems and achieve better results.

Firstly, there should be created harmonized international standards for protecting information.¹⁴⁵⁶ Because different countries have varying privacy policies, multinational companies and governing bodies encounter certain difficulties when trying to clarify the situation and decide upon appropriate actions. With the adoption of a single international standard or treaty concerning privacy

¹⁴⁵³ Frank Pasquale, *The Black Box Society* 3–10 (2015).

¹⁴⁵⁴ Daniel J. Solove & Paul M. Schwartz, *Information Privacy Law* 450–60 (7th ed. 2021).

¹⁴⁵⁵ Shoshana Zuboff, *The Age of Surveillance Capitalism* 8–12 (2019).

¹⁴⁵⁶ Graham Greenleaf, *International Data Privacy Agreements*, 163 *Privacy Laws & Bus. Int'l Rep.* 1 (2020).

protection, it will be possible to avoid conflicting jurisdictions and achieve better results.¹⁴⁵⁷

Finally, domestic data protection regulations should be harmonized with international ones. It means that all the parties should adopt legislation that guarantees sufficient protection of private information and, at the same time, does not contradict other countries' rules. Implementation of international privacy policies and compliance with relevant international standards is also necessary.

Improvement on the aspect of transparency and accountability is necessary. Users need to be informed in clear terms how their personal data is being gathered, used, retained, and transferred by multinational technological firms.¹⁴⁵⁸ More personal privacy is expected for individuals through their right to access, modification, deletion, and retraction of consent.

It can be concluded that the development of international data governance policy involves concerted global action and regulation, technology, and safeguarding of individual privacy rights in this dynamic digital age.

PART 8

CONCLUSION

It can be said that the fast development of technologies, Internet communications, cloud computing, and international digital platforms made personal information one of the most valuable resources nowadays. Along with that, issues like personal information protection, cybersecurity, and surveillance raise concerns, which leads to the importance of the question of data governance and personal data protection both on the national and international levels.

The research conducted focused on the notion of personal data protection and the features associated with cross-border personal data transfers. The main approaches to data regulation used in the European Union, the

United States, and India were considered as well as the role of various bodies involved in the process of data regulation at the international level.

To summarize, it can be stated that the problem of international data protection in the digital era is an important topic for discussion in terms of the global community as a whole.¹⁴⁵⁹ Moreover, with the constant changes in the field of information protection, future international data governance requires the use of appropriate mechanisms developed by states collaboratively.

¹⁴⁵⁷ Organisation for Economic Co-operation and Development (OECD), OECD Digital Economy Outlook 2020 210–15 (2020).

¹⁴⁵⁸ General Data Protection Regulation, Regulation (EU) 2016/679, arts. 12–14, 2016 O.J. (L 119) 1.

¹⁴⁵⁹ Christopher Kuner, Transborder Data Flows and Data Privacy Law 210–18 (2013).