INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

 ISSN:2582-6433

DISCLAIMER

 ISSN:2582-6433

EDITORIALTEAM

EDITORS

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur.Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time &Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

 ISSN:2582-6433

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

 ISSN:2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

 ISSN:2582-6433

EVALUATING CHALLENGES IN PROTECTION OF DIGITAL TRADEAND TRANSACTIONS THROUGH CYBERSPACE IN PERSPECTIVEOF PRIVATE INTERNATIONAL LAW

AUTHORED BY: SHUBHAM DIWATE[1]
IILM University, Gurugram

Abstract:

In today's globalizing cyber world, while creating and executing activities related to trade on international scale one needs to understand challenges in order to protect trade and transactions through cyberspace is need of hour. Through this paper ideal challenges of protecting Digital Trade and Transactions will be highlighted with probable solutions. While dealing with Internationally, information about transactions resides in fragmented pockets within business and government systems. The lack of safety, security, jurisdictional issues, compliance, transaction monitoring and commercial risks are the major concerns. This research paper will give you that analytical understanding and best possible solutions of real-time challenges which we faceduring transactional activities.

Keywords: Digital Trade, Cyberspace, Information Technology, InternationalTrade, Globalization, Compliance, Monitoring.

Introduction:

This paper contributes knowledge about understanding challenges in protection of Digital Trade and Transactions through Cyberspace alongwith it's evaluation. The rapid expansion of digital technologies and the internet has revolutionized global commerce, giving rise to a new era of digital trade and transactions. This transformation has brought unprecedented opportunities for businesses and consumers alike, enabling seamless cross-border transactions and fostering global economic integration. The borderless nature of cyberspace has also presented significant challenges to the traditional frameworks of Private International Law,

[1] The author is Researcher Student of Master of Laws in Department of Law, IILM University Gurugram.

 ISSN:2582-6433

which have historically beengrounded in territorial jurisdiction and state sovereignty.

As the digital economy continues to grow, it becomes increasingly crucial to address the legal complexities arising from cross-border electronic commerce, data flows, and digital services. Theintersection of cyberspace and Private International Law raises fundamental questions about jurisdiction, applicable law, and the enforcement of judgments in a virtual environment that often defies geographical boundaries. This research paper aims to evaluate the key challenges in protecting digital trade and transactions through cyberspace from the perspective of Private International Law.

Let us understand, Cyberspace, Digital trade and transactions:

Cyberspace refers to the virtual, interconnected environment created by computer networks, particularly the internet. This digital realm facilitates electronic communication, information exchange, and online interactions on a global scale. It enables instant connectivity, allowing people to communicate, share data, conduct business, and form virtual communities irrespective of physical location. As technology advances, cyberspace continues to expand, bringing new opportunities and challenges in areas such as e-commerce, cloud computing, and cybersecurity.[2]

Digital trade and transactions refer to the exchange of goods, services, and financial assets through electronic means, primarily over the internet and other digital networks. This modern form of commerce encompasses a wide range of activities, including e-commerce, online banking, digital content streaming, and cross-border data flows. It has revolutionized traditional business models, enabling companies to reach global markets more easily and consumers to access a broader range of products and services. Digital trade has significantly reduced transaction costs, increased market efficiency, and fostered innovation across various sectors. However, it also presents challenges related to cybersecurity, data privacy, and regulatory frameworks across different jurisdictions.[3]

The protection of digital trade and transactions in cyberspace faces numerous challenges due to the complex and evolving nature of the digital ecosystem. Key issues include cybersecurity threats, such as data breaches, identity theft, and financial fraud, which can undermine trust in digital platforms and cause significant economic losses. The global nature of cyberspace

[2] Gibson, 1984; Benedikt, 1991; Dodge & Kitchin, 2001.
[3] OECD, 2019; WTO, 2018; López González & Ferencz, 2018.

 ISSN:2582-6433

complicates legal and regulatory frameworks, as different jurisdictions may have conflicting laws regarding data protection, intellectual property rights, and cross-border transactions. Additionally, the rapid pace of technological innovation often outstrips the ability of regulatory bodies to develop appropriate governance structures. Privacy concerns and the ethical use of personal data present ongoing challenges, particularly as artificial intelligence and big data analytics become more prevalent in digital trade. Furthermore, the digital divide between developed and developing countries can lead to unequal participation in the global digital economy, raising issues of fairness and inclusivity.[4]

Problem Statement:

Need of Evaluating Challenges related to Digital Trade and Transactions:

- **What are the key challenges in applying Private International Law principles to protect digital trade and transactions in cyberspace, and how can these challenges be addressed to ensure effective legal protection across jurisdictions?**

A. How do jurisdictional issues in cyberspace impact the enforcement of digital trade contracts under Private International Law?
B. What are the primary obstacles in harmonizing data protection laws for cross-border digital transactions, and how can Private International Law principles be adapted to address these challenges?
C. To what extent can existing Private International Law frameworks adequately protect parties involved in digital trade, and what reforms are necessary to address emerging cybersecurity threats?

Methodology:

Given the nascent stage of knowledge on Cyberspace, through this paper have approached my research objective using a method similar to analytic induction[5]. Analytical Induction starts deductively, within the formulation of a guiding framework that is empirically validated and extended by an analysis of case data. In this study, I have analyzed three aspects of Digital Worldwhich have international significance (Digital Trade, Transactions and Cyberspace) as a general theoretical framework for analyzing cases from eyes of Private International Law to establish therelevant evaluations.

[4] UNCTAD, 2021; Meltzer, 2019; OECD, 2020
[5] Anwarul Yaquin, Legal Research and Writing Methods, Lexis Nexis

 ISSN:2582-6433

A. *Jurisdiction Issues in Cyberspace*

The borderless nature of the internet often makes it difficult to determine which court has the authority to hear a case, as parties, servers, and transactions may span multiple countries. This uncertainty can lead to conflicts of laws, where different jurisdictions have contradictory regulations regarding digital trade, further complicating the resolution of disputes. The global reach of cyberspace also enables "forum shopping," where parties may seek to litigate in jurisdictions most favorable to their case, potentially leading to unfair advantages. Even when a court claims jurisdiction and renders a judgment, enforcing that decision in another country where the defendant's assets are located can be problematic, asdemonstrated in cases like *Google LLC v. Equustek Solutions Inc*[6]. The rise of digital assets and online dispute resolution mechanisms further challenges traditional notions of jurisdiction.

The basic problems of jurisdiction in international laws and domestic laws because of it'sde-territorial nature. As a result, courts and legislators worldwide are grappling with the need to adapt existing legal principles or develop new approaches to establish clear, fair, and enforceable jurisdictional rules in cyberspace, balancing the interests of state sovereignty, individual rights, and the need for a predictable legal environment for digital trade and commerce.

B. *Primary Obstacles for cross-border transactions*

Legal and regulatory institutions encounters a significant challenge, as different countriesand regions have diverse approaches to data protection, privacy, and digital transactions, creating a lack of uniformity that complicates cross-border data flows. Differing cultural and societal values regarding privacy and the balance between individual rights and state interests make it difficult to establish universally accepted standards. The rapid pace of technological advancements often outstrips the ability of legal frameworks to adapt,creating regulatory gaps. Data localization requirements in some countries, mandating certain types of data be stored within their borders, can conflict with the global nature of digital transactions.

Private International Law principles can be adapted to address the challenges of data protection

[6] Google LLC v. Equustek Solutions Inc. (2017, Supreme Court of Canada)

 ISSN:2582-6433

laws for cross-border digital transactions in several ways. First, developing flexible conflict-of-laws rules that account for the dynamic nature of digital transactions can help determine applicable law based on factors like the location of data subjects, controllers, and processing activities. Enhancing international cooperation mechanisms for cross-border collaboration among data protection authorities can facilitate information sharing and joint investigations. Establishing global data protection standards can serve asa baseline for national laws while allowing for regional variations. Encouraging the use ofcontractual choice-of-law provisions can provide clarity in governing law and jurisdictionfor data protection matters. Creating specialized international dispute resolution mechanisms, such as arbitration or mediation processes, can address data protection and digital transaction disputes more effectively. Promoting regulatory convergence through dialogue and cooperation among lawmakers and regulators can help align data protection approaches and reduce conflicts between legal systems. Adopting technology-neutral legalprinciples that focus on outcomes and protections rather than specific technologies can provide greater flexibility as technology evolves. Finally, incorporating data protection bydesign principles into the development of digital services and technologies can reduce theneed for complex legal interventions and promote a more proactive approach to addressingcross-border data protection challenges.

C. Reforms to address cybersecurity threats

The frameworks' effectiveness is limited when dealing with emerging cybersecuritythreats, as these often exploit the gaps between national legal systems and the global natureof the internet. To address these shortcomings, several reforms are necessary. First, there'sa need for updated and harmonized rules on jurisdiction and applicable law that specificallyaccount for digital contexts, including cloud computing and decentralized technologies. Second, mechanisms for rapid and efficient cross-border enforcement of judgments relatedto cybersecurity breaches must be strengthened. Third, the development of international standards for cybersecurity measures in digital trade should be prioritized to ensure a baseline of protection across jurisdictions. Fourth, legal frameworks need to incorporate more flexible and adaptive approaches to keep pace with evolving cyber threats, possibly through the use of principles-based regulation rather than prescriptive rules. Finally, enhanced international cooperation in investigation and prosecution of cybercrime is mcrucial, including improved information sharing protocols and mutual legal assistancetreaties tailored to the digital age.

 ISSN:2582-6433

Literature Review:

Review No. 01:

Title of the Paper: How Digital Trade is Transforming GlobalizationName of the Author: Susan Lund and James Manyika

Month and Year of Publication: January 2016

Name of the Publisher: International Centre for Trade and Sustainable Development (ICTSD) andWorld Economic Forum

Summary: The spread of digital technologies is transforming global flows of goods, services, money, and people. Digital trade represents an important, albeit hard-to-measure, component of these global flows. As digital trade grows, develops, and assumes new forms, it is both facilitating globalization and transforming it. This paper examines three ways this transformation process is taking place: through cross-border flows of purely digital goods; by using "digital wrappers" to enable physical flows of goods, anessential component of the "Internet of Things"; and through the creation of online platforms for production, exchange, and consumption. Large and small companies, as well as individual entrepreneurs and consumers, in both developed economies and theemerging world will be increasingly affected by these developments, which constituteboth an opportunity and a competitive challenge. For governments and policymakers, the rapid transformation of digital trade raises important issues that will need to be addressed, including lingering barriers to its growth, appropriate ways of measuring it,and questions about governance and data security.

Review No. 02:

Title of the Paper: Digital Trade: Developing A Framework for AnalysisName of the Author: Javier López González Marie-Agnes Jouanjean Month and Year of Publication: July 2017

Name of the Publisher: OECD Trade Policy Papers No. 205

Summary: This paper explores the definition, measurement, and policy implications of digital trade, proposing a tentative typology of digital trade that can be used to unpack transactions and analyse the issues. Digitalisation is changing what and how we trade:from digital delivery to greater physical trade enabled by digital connectivity. Online platforms mean more small packages crossing borders, while new technologies are changing how services are produced and delivered. Underpinning digital trade is the movement of data: data is a means of production, an asset that can itself be traded, andthe means through which some services are traded and GVCs are organized. While there is no single definition of digital trade, there is a

growing consensus that it encompasses digitally enabled transactions in trade in goods and services which can beeither digitally or physically delivered involving consumers, firms and governments. Unpacking trade transactions along these lines using a tentative typology can help in understanding and identifying issues. For example, measuring digital trade poses challenges ranging from identifying transactions that are digitally enabled to thesectoral classification of services in a transaction, and efforts are underway to better reflect digital trade in trade statistics. For trade policy, the increased bundling of goodsand services raises issues about which trade rules (GATT or GATS) apply; trade facilitation is ever more critical for just-in-time delivery and GVCs; and the role of dataflows in enabling digital trade may require further attention, along with how to ensurethat the gains from digital trade are inclusive, within and across countries.

Review No. 03:

Title of the Paper: A Systematic Framework to Understand Transnational Governance for Cybersecurity Risks from Digital Trade

Name of the Author: Keman Huang (Renmin University of China and MIT); Stuart Madnick (Nazli Choucri MIT); Fang Zhang (Tsinghua University, and Harvard University)

Month and Year of Publication: January 2021Name of the Publisher: Wiley

Summary: Governing cybersecurity risks from digital trade is a growing responsibility for governments and corporations. This study develops a systematic framework to delineate and analyze the strategies that governments and corporations take to addresscybersecurity risks from digital trade. It maps out the current landscape based on a collection of cases where governments and corporations interact to govern transnational cybersecurity risks. This study reveals that: first, governing cybersecurityrisks from digital trade is a global issue whereby most governments implement policieswith concerning that the cybersecurity risks embedded with in purchasing transnationaldigital products can influence their domestic political and societal systems. Second, governments dominate the governance interactions by implementing trade policies whereas corporations simply comply. Corporations do, however, have chances to take more active roles in constructing the governance system. Third, supply chain cybersecurity risks have more significant impacts on governance mode between governments and corporations where as concerns on different national cybersecurity risks do not. Fourth, the interactions between governments and corporations reveal the existence of loops that can amplify or reduce cybersecurity risks. This provides policyimplications on transnational cyber security governance for policymakers and businessleaders to consider their potential options

and understand the global digital trade environment when cybersecurity and digital trade overlap.

Review No. 04:

Title of the Paper: Defining Cybersecurity Law

Name of the Author: Jeff Kosseff (Assistant Professor of Cybersecurity Law, United States Naval Academy. J.D., Georgetown University Law Center; M.P.P., B.A., University of Michigan).

Name of the Publisher: Iowa Law Review

Summary: This Article aims to fill that gap by defining "cybersecurity law." Although many articles have addressed various aspects of cybersecurity, none has stepped back to define exactly what "cybersecurity" is and the goals of statutes and regulations that aimto promote cybersecurity. By defining the scope and goals of this new legal field, policymakers can then examine how lawmakers could improve existing laws. Part II ofthis Article briefly describes the cybersecurity challenges that the United States faces by examining the cyberattack on Sony Pictures Entertainment. Part III defines "cybersecurity law" as a legal framework that "promotes the confidentiality, integrity, and availability of public and private information, systems, and networks, through theuse of forward-looking regulations and incentives, with the goal of protecting individual rights and privacy, economic interests, and national security." Part IV explains the current legal regime for cybersecurity and concludes that many of the most prominent cybersecurity laws only address a small portion of the broader legal framework. Part V examines the gaps in current U.S. cybersecurity law and suggests starting points for improvements.

Review No. 05:

Title of the Paper: Cybersecurity Issues and Challenges: In Brief

Name of the Author: Eric A. Fischer Senior Specialist in Science and TechnologyMonth and Year of Publication: August 12, 2016

Name of the Publisher: Congressional Research Service

Summary: The federal role in cybersecurity involves both securing federal systems and assisting in protecting nonfederal systems. Under current law, all federal agencies have cybersecurity responsibilities relating to their own systems, and many have sector- specific responsibilities for CI. On average, federal agencies spend more than 10% of their annual ICT budgets on cybersecurity. More than 50 statutes address various aspects of cybersecurity. Five

 ISSN:2582-6433

bills enacted in the 113th Congress and another in the 114th address the security of federal ICT and U.S. CI, the federal cybersecurity workforce, cybersecurity research and development, information sharing in both the public and private sectors, and international aspects of cybersecurity. Other bills considered by Congress have addressed a range of additional issues, including data breach prevention and response, cybercrime and law enforcement, and the Internet of Things, among others. Among actions taken by the Obama Administration during the 114th Congress are promotion and expansion of nonfederal information sharing and analysis organizations; announcement of an action plan to improve cybersecurity nationwide; proposed increases in cybersecurity funding for federal agencies of more than 30%, including establishment of a revolving fund for modernizing federal ICT; and a directive laying out how the federal government will respond to both government and private-sector cybersecurity incidents. Those recent legislative and executive- branch actions are largely designed to address several well-established needs in cybersecurity. However, those needs exist in the context of difficult long-term challenges relating to design, incentives, consensus, and environment. Legislation andexecutive actions in the 114th and future Congresses could have significant impacts onthose challenges.

Challenges In Protecting Digital Trade And Transactions Through Cyberspace:

The relationship between cyberspace and private international law is complex and evolving, as theborderless nature of the digital realm challenges traditional notions of jurisdiction and applicable law.

"Private international law, also known as conflict of laws, deals with legal disputes involving foreign elements, and its principles are increasingly tested inthe context of cyberspace."

The internet's global reach often results in cross-border transactions, interactions, and disputes, raising questions about which country's laws apply and which courts have jurisdiction. This intersection creates challenges in areas such as e-commerce, intellectual property rights, data protection, and online defamation. Courts and legislators worldwide are grappling with adapting existing legal frameworks or developing new ones to address issues like online consumer protection, digital contracts, and cybercrime that transcend national boundaries. The ongoing debate centers on balancing the need for legal certainty and predictability with the dynamic and transnational nature of cyberspace activities, often leading to complex legal analyses and potentialconflicts between different legal systems.

 ISSN:2582-6433

Challenges in protecting digital trade and transactions through cyberspace are numerous and complex, stemming from the rapidly evolving nature of technology and the global scale of digitalcommerce. These challenges include:

1. **Cybersecurity Threats**: The increasing sophistication of cyberattacks, including data breaches, ransomware, and financial fraud, poses significant risks to digital trade (Verizon, 2021).
2. **Regulatory Fragmentation**: Inconsistent legal frameworks across jurisdictions create compliance challenges for businesses operating globally (OECD, 2019).
3. **Data privacy Concerns**: Balancing data protection with the free flow of information necessary for digital trade is an ongoing challenge (Aaronson & Leblond, 2018).
4. **Cross-border Enforcement**: Difficulties in enforcing laws and regulations across national boundaries complicate efforts to combat cybercrime (UNODC, 2020).
5. **Technological Complexity**: Rapid advancements in technology, such as AI and IoT, create new vulnerabilities and challenges for security measures (World Economic Forum, 2020).
6. **Digital divide**: Inequalities in access to digital infrastructure and skills hinder inclusive participation in the digital economy (ITU, 2021).
7. **Intellectual Property Protection**: Safeguarding intellectual property rights in the digital realm remains a significant challenge (WIPO, 2020).
8. **Trust and Authentication**: Ensuring secure and reliable authentication methods for digital transactions is crucial but challenging (Deloitte, 2019).
9. **Emerging Technologies**: The integration of blockchain, quantum computing, and other emerging technologies introduces new security paradigms and potential vulnerabilities (IEEE, 2020).
10. **State-sponsored Cyber Activities**: Geopolitical tensions manifesting in cyberspace can disrupt digital trade and compromise security (CSIS, 2021).

*<u>*Please check References mentioned in Appendix A.*</u>

- Here's a list of challenges in the protection of digital trade and transactions throughcyberspace:

Cybersecurity Threats	a) Data breaches b) Ransomware attacks

 ISSN:2582-6433

	c) Phishing scams d) Malware infections e) Distributed Denial of Service (DDoS) attacks
Regulatory Fragmentation	f) Inconsistent legal frameworks across jurisdictions g) Varying data protection regulations
	h) h. Conflicting national cybersecurity standards
Data Privacy Concerns	i) Balancing data protection with free information flow j) Compliance with diverse privacy laws (e.g., GDPR, CCPA) k) Cross-border data transfer restrictions
Cross-border Enforcement	l) Jurisdictional issues in cybercrime prosecution m) Difficulty in enforcing judgments internationally n) Lack of harmonized international cybercrime laws
Technological Complexity	o) Rapid evolution of technologyoutpacing security measures p) Integration of AI and machine learningin cyber attacks q) Vulnerabilities in Internet of Things(IoT) devices
State-sponsored Cyber Activities	r) Cyber espionage targetingtrade secrets s) State-backed cyber attacks oncritical infrastructure t) Geopolitical tensions u) manifesting in cyberspace

 ISSN:2582-6433

Case Laws:

October 2023, there have been several key developments and cases in the realm of digital trade and transactions from a private international law perspective. It's important to note that jurisdictional issues and the enforcement of laws in cyberspace often present complex challenges. These cases highlight various challenges in protecting digital trade and transactions:

1. **Data Privacy and GDPR Compliance**: The General Data Protection Regulation (GDPR)has had a significant impact on international digital trade, particularly due to cross-borderdata transfer restrictions. Cases like *Schrems II* have implications for businesses globally regarding data transfer mechanisms.[7] It raised concerns about the level of protection for personal data transferred from the EU to the US. While focused on EU-US transfers, thedecision affects any country receiving EU data that doesn't meet GDPR-level protection.
2. **Jurisdictional Challenges**: Courts have dealt with the complexities of jurisdiction in cyberspace, focusing on where digital transactions are deemed to occur and which laws apply. The case of *Google LLC v. Equustek Solutions Inc*[8]. in Canada highlighted issues around global enforcement of court orders in the digital realm.
3. **E-commerce and Consumer Protection**: EU regulations have strengthened consumer rights in digital transactions, leading to case law that ensures consumer protection within international online marketplaces.
4. **Blockchain and Cryptocurrency Disputes**: Courts in several jurisdictions have begun to tackle issues related to blockchain transactions, which are inherently transnational. These cases often address both jurisdiction and the recognition of digital assets as property.
5. **Domain Name Disputes**: The Uniform Domain-Name Dispute-Resolution Policy (UDRP)remains a pivotal mechanism for resolving international disputes over domain names, illustrating the application of international principles to digital spaces.

Recent Developments:

There have been significant developments in international law, cybersecurity regulations, and digital trade agreements, reflecting the rapid evolution of digital technologies and the

[7] Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems (Schrems II) (2020, EU)
[8] Google LLC v. Equustek Solutions Inc. (2017, Supreme Court of Canada)

 ISSN:2582-6433

increasing importance of cybersecurity. Here's an overview of some key trends and developments:

- **International Law Trends**: The Tallinn Manual on the International Law Applicable to Cyber Warfare are being updated to address cyber operations. The invalidation of the EU-U.S. Privacy Shield and the enactment of the EU-U.S. Data Privacy Framework reflect continued efforts to balance cross-border data flows with privacy protections.
- **Cybersecurity Trends**: Many countries have updated or introduced comprehensive national cybersecurity strategies to address emerging threats, focusing on critical infrastructure protection and information sharing. The United Nations' Open-ended Working Group (OEWG) and the Group of Governmental Experts (GGE) continue fostering international dialogue on norms and confidence-building measures in cyberspace.
- **Digital Data Trade Agreements:** The World Trade Organization continues negotiations on e-commerce, aiming to establish global rules governing digital trade, which include dataflow facilitation and addressing barriers to digital goods and services. Initiatives like the Digital Economy Partnership Agreement (DEPA) between countries such as Chile, New Zealand, and Singapore are designed to promote digital trade standards and cooperation onissues like AI and digital identities.
- **Balancing Security and Innovation**: Policymakers strive to foster innovation while ensuring robust cybersecurity frameworks, seeking to protect economies and societies fromincreasing cyber threats.
- **Privacy and Data Sovereignty**: Stricter data protection laws and emerging frameworks aim to safeguard personal data, reflecting growing public concern over privacy.
- **Digital Inclusion**: Ensuring equitable access to digital technologies remains a priority for sustainable development, requiring international cooperation and investment in digital infrastructure.

Conclusions:

As this analysis has shown, issues of jurisdiction, applicable law, and enforcement of judgments become increasingly complex in the borderless realm of the internet. While existing legal frameworks struggle to keep pace with technological advancements, it is clear that a harmonized approach to private international law is crucial for ensuring the protection of digital

 ISSN:2582-6433

trade. Movingforward, international cooperation and the development of uniform standards will be essential in addressing these challenges effectively. Policymakers and legal scholars must continue to adapt and innovate to create a robust legal environment that fosters trust, security, and growth in the digital economy while respecting the principles of sovereignty and fairness in cross-borderdisputes.

The lack of safety, security, jurisdictional issues, compliance, transaction monitoring and commercial risks are the major concerns. The rapid expansion of digital technologies and the internet has revolutionized global commerce, giving rise to a new era of digital trade and transactions. The rise of digital assets and online dispute resolution mechanisms further challenges traditional notions of jurisdiction. Promoting regulatory convergence through dialogue and cooperation among lawmakers and regulators can help align data protection approaches and reduceconflicts between legal systems.

All research has limitations, so also my work. Most importantly, this research paper highlighted prominent challenges against protection of digital trade and transactions through cyberspace.

Appendix A

References

1. Aaronson, S. A., & Leblond, P. (2018). Another Digital Divide: The Rise of Data Realmsand its Implications for the WTO. Journal of International Economic Law, 21(2), 245-272.
2. CSIS. (2021). Significant Cyber Incidents. Center for Strategic and International Studies.
3. Deloitte. (2019). The future of authentication in financial services.
4. IEEE. (2020). IEEE International Conference on Quantum Computing and Engineering(QCE).
5. ITU. (2021). Measuring digital development: Facts and figures 2021. International Telecommunication Union.
6. OECD. (2019). Trade in the Digital Era. OECD Going Digital Policy Note.
7. UNODC. (2020). Comprehensive Study on Cybercrime. United Nations Office on Drugsand Crime.
8. Verizon. (2021). 2021 Data Breach Investigations Report.
9. WIPO. (2020). World Intellectual Property Report 2020: Innovation in the Digital

 ISSN:2582-6433

Era.World Intellectual Property Organization.

10. World Economic Forum. (2020). The Global Risks Report 2020.

Appendix B

Bibliography

1. Anwarul Yaquin, Legal Research and Writing Methods, Lexis Nexis
2. Aaronson, S. A., & Leblond, P. (2018). Another Digital Divide: The Rise of Data Realmsand its Implications for the WTO. Journal of International Economic Law, 21(2), 245-272.