REVISTA DE DIREITO INTERNACIONAL

BRAZILIAN JOURNAL OF INTERNATIONAL LAW

Editores responsáveis por essa edição:

Editores:

Nitish Monebhurrun

Ardyllis Alves Soares

Marcelo Dias Varella

Editores convidados:

David Ramiro Troitiño

Ignacio Bartesaghi

ISSN 2237-1036

Revista de Direito Internacional Brazilian Journal of International Law	Brasília	v. 20	n. 2	p. 1-633	ago	2023

doi: 10.5102/rdi.v20i2.9154

The United Nation data governance: a panopticon and a catalyst for cooperation*

A governança de dados das Nações Unidas: um panóptico e um catalisador para a cooperação

Varda Mone**

CLV Sivakumar ***

Abstract

The rapid expansion of technology and digitization has given rise to extensive data collection, processing, and trade, triggering significant concerns regarding data privacy and security. Varying data privacy laws across jurisdictions pose complex challenges in our interconnected world. This study explores the feasibility of establishing a United Nations (UN) global data privacy authority to address these issues. Such an entity could enhance privacy protection, promote secure data storage, and facilitate international data flows. We analyze the potential benefits and obstacles, leveraging the UN's resources to adapt data protection regulations to technological advancements. A UN agency dedicated to data privacy could promote transparency and accountability, benefiting governments and enterprises. We advocate for UN involvement in International Data Governance, drawing parallels with WIPO's success in intellectual property rights. This institution, symbolically acting as a "panopticon," would oversee and regulate data practices, fostering trust and responsibility in the digital ecosystem.

Keywords: data privacy; United Nations international data governance digital economy; WIPO; global data protection.

Resumo

A rápida expansão da tecnologia e da digitalização deu origem a uma extensa recolha, processamento e comércio de dados, desencadeando preocupações significativas relativamente à privacidade e segurança dos dados. As diferentes leis de privacidade de dados entre jurisdições representam desafios complexos no nosso mundo interligado. Este estudo explora a viabilidade de estabelecer uma autoridade global de privacidade de dados das Nações Unidas (ONU) para abordar estas questões. Tal entidade poderia melhorar a protecção da privacidade, promover o armazenamento seguro de dados e facilitar os fluxos internacionais de dados. Analisamos os potenciais benefícios e obstáculos, aproveitando os recursos da ONU para adaptar as regulamentações de proteção de dados aos avanços tecnológicos. Uma agência da ONU dedicada à privacidade de dados poderia promover a transparência e a responsabilização, beneficiando governos e empresas. Defendemos o

* Recebido em 05/07/2023
Aprovado em 20/10/2023

** Presently, she is a Research Scholar at VIT-AP School of Law pursuing a PhD in Data Protection Laws. She did her graduation (B.A.LLB) from Nagpur University and Post-graduation (LLM in Constitution and Administrative Law) from Dr Ram Manohar Lohia National Law University Lucknow. She has worked as Assistant Professor at the Indore Institute of Law, Indore, M.P. She was also a full-time research intern at the Office of Mr. Vijay Sai Reddy, Member of Rajya Sabha, Indian Parliament. She is selected for international research Fellowship Research Fellowships in Humanities and Social Sciences (Remote) by University of Religions and Denominations (URD) & Central Asian Legal Research (CALR) Fellowship by Tashkent State University of Law.
Email: vardamone.21phd7055@vitap.ac.ine

*** He did his B.Com. From Nagarjuna University, A.P.in the year 1989; M.A. from Alagappa university T.N. in the year 2004; B.L. from Nagarjuna University, A.P. in the year 1994 and M.L. from Nagarjuna University, A.P. in the year 1996. He completed PhD (Law) from Nagarjuna University in 2012. He has worked as Lecturer in Law during the period 1996-1998 in SBRTM Law College, Cuddapah (A.P). and as Assistant Professor of Law in Jaya Group of Educational Institutions, Chennai, (TN) during the period 1998-2008; Later to which he worked as Associate Professor of Law in VIT Business School, VIT University, Vellore, Tamil Nadu. He served in the position of Registrar VIT-AP University from 2016 till 15 June 2022. Presently, He is a Professor of Law at VIT University, Vellore.
Email: sivakumar.clv@vit.ac.in

envolvimento da ONU na Governança Internacional de Dados, traçando paralelos com o sucesso da OMPI em direitos de propriedade intelectual. Esta instituição, agindo simbolicamente como um "panóptico", supervisionaria e regularia as práticas de dados, promovendo a confiança e a responsabilidade no ecossistema digital.

Palavras-chave: Proteção de Dados, Direito Internacional, Privacidade de Dados, Nações Unidas; Gestão de dados; Perspectiva do Terceiro Mundo.

1 Introduction

In today's fast-paced, hyperconnected world, the relentless march of technology and digitalization has fundamentally transformed the way we live, work, and interact. With every click, swipe, and tap, we generate a digital footprint, leaving behind a trail of data that paints a detailed portrait of our lives, habits, preferences, and vulnerabilities. This digital revolution has heralded unprecedented progress, powering innovation, economic growth, and global interconnectedness. However, it has also ignited a profound and pressing concern - the issue of data privacy.[1]

The rapid expansion of technology and digitization has ushered in an era of extensive data collection, processing, and trade. From our online shopping preferences to our health records, from our social media interactions to our financial transactions, an astonishing array of personal data is now being harvested, analysed, and monetized on a global scale. While this wealth of information has the potential to fuel ground breaking discoveries and advancements, it has also raised a chorus of alarms regarding data privacy and security.

As we navigate this digital landscape, we are confronted with a formidable challenge: how to safeguard the privacy of individuals and the security of their data in a world where boundaries have blurred, and data flows seamlessly across borders. The crux of this challenge lies in the stark divergence of data privacy laws and regulations from one jurisdiction to another. Varying data protection standards, conflicting legal requirements, and disparities in enforcement mechanisms have created a complex and often bewildering maze for individuals, corporations, and governments alike. Consider a scenario where an individual's personal data, residing on a cloud server located in one country, is accessed and used by a service provider headquartered in another, while the individual resides in a third country. Whose data protection laws apply? Which regulatory body has jurisdiction? How does one seek recourse in case of a breach or violation? These are just a few of the questions that underscore the multifaceted challenges posed by the global data privacy landscape.[2]

It is within this intricate web of data privacy challenges that we embark on a journey to explore the feasibility of establishing a global data privacy authority under the auspices of the United Nations (UN). Such an entity, if realized, would serve as a lighthouse amidst the turbulent seas of data governance. It would strive to harmonize data privacy regulations, advocate for secure data storage practices, and facilitate the free and secure flow of data across borders, thereby addressing the core concerns surrounding data privacy in the digital age.

Throughout this paper, we will delve into the intricacies of this proposal, scrutinizing its potential benefits, examining the obstacles it must overcome, and harnessing the UN's vast expertise and resources to pave the way for a new era in data privacy governance. In doing so, we aim to shed light on the possibilities and challenges of creating an international data privacy agency, offering insights that are informed by the evolving landscape of technology and data management. We will also draw parallels with the successful model of the World Intellectual Property Organization (WIPO), which has effectively addressed global issues related to intellectual property rights. By advocating for the United Nations to play a pivotal role in International Data Governance, we aim to contribute to the ongoing discourse on how to safeguard data privacy while harnessing the transformative potential of the digital age.[3]

It is important to note that within this exploration, we employ the term "panopticon" symbolically. It ser-

[1] UNITED NATIONS. *Data strategy of the Secretary-General for action by everyone, everywhere with insight, impact, and integrity 2020-22*. 2020. Available in: https://www.un.org/en/content/datastrategy/images/pdf/UN_SG_Data-Strategy.pdf.

[2] UNITED NATIONS. System Chief Executives Board for Coordination. *International data governance*: pathways to progress. Available in: https://unsceb.org/international-data-governance-pathways-progress. Access on: May 2023.

[3] HERT, Paul de; PAPAKONSTANTINOU, Vagelis. Three Scenarios for International Governance of Data Priv-acy: towards an International Data Privacy Organ-ization, Preferably a UN Agency?. *A Journal of Law and Policy for the Information Society,* p. 271, 2013.

ves as a metaphor for the oversight and regulation of data practices in a world where constant vigilance is required to ensure the responsible and ethical use of data by both state and non-state actors within the digital ecosystem. In the pages that follow, we will navigate the intricate terrain of data privacy, seeking to illuminate a path forward, one where technology and privacy can coexist harmoniously, and where trust and responsibility can thrive in an ever-expanding digital world.

1.1 Background and Context

The exponential growth of technology and digitization has profoundly transformed modern life. A key consequence is the exponential generation of data through online activities. This "big data" is leveraged by organizations to derive insights and optimize operations. For instance, e-commerce platforms use customer data to provide personalized recommendations. However, the data economy raises substantial privacy and security concerns. As data volume grows, so do risks of unauthorized access and breaches. The Equifax hack exemplified such dangers.[4] Furthermore, advanced algorithms like AI analyze big data to forecast and automate decisions. But their effectiveness depends on extensive data, raising ethical issues around privacy and algorithmic bias. The COVID-19 pandemic accelerated technology integration, normalizing remote work, online education, and telehealth. While upholding vital services, this increased exposure of sensitive data to cyber threats.

While data and technology offer opportunities, their exponential growth also surfaces apprehensions around privacy, security, and ethical use of algorithms. As technology continues transforming society, solutions must emerge to harness its benefits while adequately addressing its risks. Achieving the right balance will enable realizing technology's promise while protecting users and ethical values. But continued vigilance is required to ensure trust in an increasingly digitized world. Furthermore, the global nature of data flows and technology complicates regulatory approaches, as differing data privacy laws across jurisdictions create complexities for compliance.

[4] BERGHEL, H. The equifax hack revisited and repurposed. *Computer*, v. 53, n. 5, p. 85, 2020.

1.2 The Complexity of Varying Data Privacy Laws Across Jurisdictions

The complexity of varying data privacy laws across jurisdictions is a significant challenge in the digital age. Different countries and regions have established their own regulations and frameworks to govern data protection, often resulting in a patchwork of conflicting laws and requirements. This fragmentation poses considerable difficulties for individuals, corporations, and governments that operate in a globalized world.[5]

One notable example is the European Union's General Data Protection Regulation (GDPR), which came into effect in 2018.[6] GDPR is one of the most comprehensive data protection laws globally and sets stringent standards for the collection, processing, and storage of personal data. GDPR applies not only to EU-based companies but also to any organization worldwide that processes the data of EU residents. This extraterritorial reach created significant compliance challenges for multinational corporations.

To navigate this complexity, the EU and the United States negotiated the EU-US Privacy Shield framework[7]. This agreement aimed to facilitate the transfer of personal data between the EU and the US by providing a mechanism for US companies to demonstrate GDPR compliance. However, in July 2020, the European Court of Justice invalidated the Privacy Shield[8], citing concerns about US government surveillance practices. This ruling further underscored the complexities of cross-border data protection and the need for robust international agreements.[9]

Since then, the EU and the US have been working on a new framework for transatlantic data flows, called the EU-US Data Privacy Framework (DPF).[10] The DPF

[5] CORTEZ, E. K. (ed.). Data protection around the world: privacy laws in action. *Springer Nature*, 20 Nov. 2020.

[6] General Data Protection Regulation, 2018.

[7] EUROPEAN UNION. Department of Commerce and the European Commission, UK Government, and Swiss Federal Administration. *Privacy Shield Framework*. Available in: https://www.privacyshield.gov/ps/eu-us-framework.

[8] EUROPEAN UNION. Court of Justice of the European Union. *Data protection commissioner v Facebook Ireland and Maximillian Schrems C-311/18*. 2020.

[9] YAKOVLEVA, Svetlana; IRION, Kristina. Pitching trade against privacy: reconciling EU governance of personal data flows with external trade. *International Data Privacy Law*, v. 10, n. 3, 2020.

[10] EUROPEAN UNION. Department of Commerce and the European Commission, UK Government, and Swiss Federal Admin-

is meant to replace the Privacy Shield and address the points raised by the court in its Schrems II decision[11]. On October 7, 2023, US President Biden signed an Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities, which introduced new binding safeguards to limit the access of US intelligence agencies to EU data and established an independent and impartial redress mechanism for Europeans.[12] On July 10, 2023, the European Commission adopted its adequacy decision for the DPF, which concluded that US data protection laws offer an adequate level of protection for European citizens. The DPF is expected to provide legal certainty and facilitate cross-border commerce between the EU and the US, while respecting the fundamental rights of individuals.[13]

Another instance is the contrasting data privacy laws between the EU and China. While the EU emphasizes strong data protection rights and consent-based data processing, China has enacted laws that grant the government broad access to data for security and surveillance purposes. This disparity in approaches poses challenges for international businesses operating in both regions, as they must reconcile conflicting requirements. Moreover, the emergence of new data privacy laws in various jurisdictions, such as the California Consumer Privacy Act (CCPA) in the United States and the Personal Information Protection Law (PIPL) in China, adds another layer of complexity. Companies that operate globally must comply with multiple, often divergent, legal frameworks.[14]

Another development in this area is the release of the draft Provisions on Regulating and Promoting Cross-Border Data Flows by China's data protection regulator, the Cyberspace Administration of China (CAC), on September 28, 2023.[15] The draft Provisions propose a number of exemptions for businesses that would otherwise be subject to the existing data export restrictions under the PIPL, such as those that expect to export personal information of less than 10,000 individuals from China within one year, or those that need to transfer data for contractual. The draft Provisions also introduce a certification mechanism for cross-border data transfers, which would allow certified organizations to bypass the security assessment process required by the PIPL. These proposed changes are expected to ease some of the compliance burdens for international businesses operating in China, and to promote cross-border data flows while ensuring data security and privacy. However, some experts have also pointed out that there are still some ambiguities and uncertainties in the draft Provisions, such as the definition of "necessity" for data transfers, the scope and criteria of certification, and the potential conflicts with other existing or upcoming regulations. Therefore, it remains to be seen how the final version of the Provisions will address these issues and how it will align with other data protection regimes, such as the GDPR.[16]

The complexity of global data transfer and multiple data protection laws has led to Several court cases like-firstly, The Schrems II case is a pivotal example that underscores the challenges associated with cross-border data transfers. Max Schrems, a privacy activist, raised concerns about the validity of Standard Contractual Clauses (SCCs) as a mechanism for transferring personal data from the European Union (EU) to third countries. SCCs are legal contracts that require data exporters and importers to adhere to EU data protection standards. The case brought into question whether SCCs provided adequate safeguards against US government surveillance.[17] The European Court of Justice (ECJ) ruled in 2020 that SCCs were generally valid. However, they could only be relied upon if data protection authorities suspended or prohibited data transfers when the level of protection in the third country did not meet EU standards. This ruling adds an additional layer of complexity for companies relying on SCCs for international

istration. *Privacy Shield Framework*. Available in: https://www.privacyshield.gov/ps/eu-us-framework.

[11] TRACOL, Xavier. Schrems II: the return of the Privacy Shield. *Computer Law & Security Review*, v. 39, 2020.

[12] EUROPEAN COMMISSION. *Questions & answers*: EU-US data privacy framework. 2023. Available in: https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_3752.

[13] EUROPEAN COMMISSION. *Questions & answers*: EU-US data privacy framework. 2023. Available in: https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_3752.

[14] ZHENG, G. Trilemma and tripartition: the regulatory paradigms of cross-border personal data transfer in the EU, the US and China. *Computer Law & Security Review*, 2021.

[15] CASALINI, F.; GONZÁLEZ, J. L. *Trade and cross-border data flows*. 2019.

[16] ZHENG, G. Trilemma and tripartition: the regulatory paradigms of cross-border personal data transfer in the EU, the US and China. *Computer Law & Security Review*, 2021.

[17] COMPAGNUCCI, M. Corrales; ABOY, M.; MINSSEN, T. *Cross-border transfers of personal data after Schrems II*: supplementary measures and new standard contractual clauses (SCCs). 2021.

data transfers, as it requires ongoing assessments of the data protection landscape in recipient countries.[18]

Secondly, The Microsoft v. United States[19] case highlights the extraterritorial reach of data privacy laws and their potential clash with national sovereignty. The case revolved around access to data stored on Microsoft servers located outside the United States. US law enforcement sought access to this data under a warrant, but Microsoft contested the request, arguing that the warrant did not apply to data stored abroad. Before the US Supreme Court could issue a ruling, the passage of the Clarifying Lawful Overseas Use of Data Act (CLOUD Act) in 2018 fundamentally altered the landscape. The CLOUD Act granted US authorities the authority to compel US-based companies to disclose data stored abroad, emphasizing the global reach of US data privacy laws. This shift poses challenges for international companies as they must comply with US laws that now extend beyond US borders.[20]

Thirdly, The Facebook v. Belgium case delves into the complexities of jurisdictional disputes and enforcement of data privacy laws across borders. In this case, the Belgian Data Protection Authority (DPA) ordered Facebook to halt its tracking of non-Facebook users in Belgium without their consent, under the threat of substantial fines. Facebook contended that it was subject to Irish law, given its European headquarters' location. The Court of Justice of the European Union (CJEU) ultimately ruled in 2019 that national Data Protection Authorities (DPAs) could act against companies like Facebook, even if they were not the lead supervisory authority under the GDPR. This ruling exemplifies how EU data protection laws grant individual member states the authority to enforce GDPR provisions, resulting in potential legal disputes and divergent interpretations across borders.[21]

Therefore, the evolving landscape of data privacy laws across jurisdictions presents an intricate tapestry of regulations, agreements, and court rulings. Businesses operating on a global scale must continuously adapt to these complexities, ensuring compliance with a patchwork of laws while safeguarding the privacy rights of individuals. As international data privacy frameworks continue to evolve, staying abreast of legal developments and seeking legal counsel remains crucial for businesses to navigate this intricate terrain effectively.

In response to these challenges, there is a growing recognition of the need for international cooperation and harmonization of data privacy laws. Organizations like the United Nations are exploring the feasibility of establishing a global data privacy authority to address these issues. Such an entity could work toward creating a common framework that respects privacy rights while facilitating the responsible and secure flow of data across borders. Achieving this delicate balance is essential to harnessing the benefits of technology expansion and digitization while safeguarding data privacy and security in our interconnected world.

2 Research Objectives

2.1 Enhancing Privacy Protection and Promoting Secure Data Practices

In this research objective, our aim is to qualitatively assess how the establishment of a United Nations (UN) global data privacy authority can significantly enhance privacy protection and promote secure data storage practices. To substantiate these arguments, we draw upon real-life examples that underscore the critical need for such an entity. A prime illustration of the need for enhanced privacy protection is the European Union's General Data Protection Regulation (GDPR), which was enacted in 2018. GDPR introduced rigorous standards for the protection of personal data, including principles of data minimization, purpose limitation, and secure processing. By examining the substantial impact of GDPR on privacy protection within the EU and beyond, we underscore the positive outcomes achievable through robust data privacy regulations.

Moreover, recent data breaches, such as the Equifax breach in 2017[22], serve as stark reminders of the perils

[18] STREINZ, T. The evolution of European data law. *In*: CRAIG, Paul; BÚRCA, Gráinne de (ed.) *The Evolution of EU Law'OUP*. 3rd. ed. Oxford: Oxford University Press, 2021.

[19] United States v. Microsoft Corp., 584 U.S. 138 S. Ct. 1186 (2018).

[20] HICKOK, Elonnai; KHARBANDA, Vipul. *An Analysis of the CLOUD Act and Implications for India*. 2018.

[21] STAFF, Reuters. *Facebook loses Belgian privacy case, faces fine of up to $125 million*. Available in: https://www.reuters.com/article/us-facebook-belgium-idUSKCN1G01LG.

[22] BERGHEL, H. The equifax hack revisited and repurposed. *Computer*, v. 53, n. 5, p. 85, 2020.

of inadequate data security measures. These real-world incidents highlight the urgent necessity for secure data storage practices. Through qualitative analysis, we can delve into the repercussions of such breaches, emphasizing the importance of stringent data security measures advocated by a UN global data privacy authority. By examining these case studies and employing qualitative analysis, we elucidate how the proposed UN authority can play an active and indispensable role in enhancing privacy protection and instigating secure data practices on a global scale.

2.2 Facilitating International Data Flows in the Digital Age

This research objective is dedicated to analyze how a UN global data privacy authority could effectively facilitate the secure and seamless exchange of data across borders in the digital age. To substantiate our arguments, we draw insights from recent developments and real-life examples that highlight the intricacies of international data flows and underscore the compelling need for international cooperation. A salient example is the EU-US Privacy Shield framework, which exemplifies the challenges associated with international data transfers and the complexities stemming from conflicting data protection regulations. By delving into the history of the Privacy Shield, its subsequent invalidation by the European Court of Justice, and the ongoing efforts to establish the EU-US Data Privacy Framework, we illuminate the pressing need for a harmonized approach to international data flows.[23]

Additionally, we throw light on the disparities in data privacy laws between regions such as the European Union and China. These divergent approaches to data protection create compliance hurdles for multinational corporations. By meticulously examining these disparities and their tangible effects on cross-border data flows, we emphasize the relevance and urgency of a UN global data privacy authority in bridging gaps and fostering international cooperation.[24] Furthermore, we illustrate the evolving landscape of data regulation. While these provisions aim to alleviate compliance burdens and promote cross-border data flows, they also reveal ambiguities and uncertainties, underlining the imperative for a unified global approach to data privacy.

In this research paper, utilizing the context of these real-world cases, we offer an in-depth analysis of how a United Nations (UN)-led initiative can serve as a robust framework for enabling seamless international data transfers while simultaneously upholding data security and privacy. This initiative aims to address the challenges posed by our increasingly interconnected global landscape, characterized by the pervasive influence of digitalization and the rapid expansion of technology. In a manner akin to the pioneering role of the World Intellectual Property Organization (WIPO) in effectively managing cross-border issues related to intellectual property, we explore the potential for the UN to play a similar role in the realm of data governance.

3 Data Privacy in the Digital Age

In our exploration of the potential establishment of a United Nations (UN) global data privacy authority, we have uncovered critical insights into how such an initiative could enhance privacy protection, promote secure data practices, and facilitate international data flows. These research objectives have provided us with a comprehensive understanding of the challenges and opportunities in our increasingly interconnected global landscape, characterized by the proliferation of technology and digitalization.

3.1 The Proliferation of Technology and Digitalization

The proliferation of technology and digitalization has reshaped nearly every aspect of human existence. This transformative wave of innovation has left an indelible mark on the way we live, work, communicate, and even perceive reality. At the core of this seismic shift lies an intricate relationship between technology, data, and our understanding of privacy.

Data Explosion and Collection: One of the defining features of the digital age is the astounding volume of data generated and collected daily. This explosion of data is fuelled by a multitude of sources, ranging from smar-

[23] EUROPEAN COMMISSION. *Data protection*: European Commission adopts new adequacy decision for safe and trusted EU-US data flows. 2023. Available in: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721.

[24] Data Protection Regulations and International Data Flows: Implications for Trade and Development (UNC-TAD 2016).

tphones and wearable devices to sensors embedded in everyday objects. Social media platforms, e-commerce websites, and online services also contribute significantly to the continuous stream of information. Every click, swipe, purchase, or social interaction leaves a digital footprint, accumulating in vast reservoirs of data.[25] This data is incredibly diverse, encompassing personal information, preferences, behaviours, and even intimate details of individuals' lives. The sheer scale and diversity of data collected in the digital age are unparalleled in human history.[26]

Data Processing and Analysis: Simultaneously, technological advancements in data processing and analysis have unlocked the potential of this data deluge. Artificial intelligence (AI), machine learning, and big data analytics have ushered in an era of data-driven decision-making. These technologies can sift through massive datasets at remarkable speeds, identifying patterns, trends, and correlations that would be impossible for humans to discern.

The implications of this are far-reaching. In healthcare, AI can assist in diagnosing diseases and predicting patient outcomes by analysing medical records and imaging data. In finance, predictive analytics can help identify fraudulent transactions or assess credit risk. In marketing, personalization algorithms can tailor advertisements to individual consumer preferences. However, as data becomes increasingly central to decision-making, concerns about privacy and security loom large.

Data as a Commodity: The digital age has given rise to a novel economic paradigm where data has become a valuable commodity. Data brokers, advertisers, and tech giants amass vast fortunes by trading in personal information. User profiles are created, refined, and sold to the highest bidder. Advertisers use this data to deliver hyper-targeted advertisements, and companies use it to gain a competitive edge.

This commodification of data raises significant ethical questions. Users often have limited control over how their data is used and shared, and they may not fully grasp the extent to which their information is bought and sold. The monetization of personal data can lead to a loss of individual autonomy and privacy, prompting calls for more stringent regulations and consumer protections.

Privacy and Security Concerns: Amid this digital revolution, data privacy and security have become paramount concerns. The interconnectedness of the digital world has made data vulnerable to cyberattacks and breaches. Hackers, criminal organizations, and state-sponsored actors exploit security weaknesses to gain unauthorized access to sensitive information. High-profile data breaches, such as the Equifax breach in 2017[27], have exposed the personal data of millions of individuals, underscoring the urgency of protecting data in the digital age.

Moreover, the lack of privacy awareness among the general public is a pressing issue. Many individuals are unaware of the extent to which their data is collected and how it is used. Privacy policies and consent forms, often laden with legal jargon, make it challenging for people to make informed choices about their data. This lack of transparency erodes trust and undermines the principles of informed consent.

In this landscape, navigating the complex web of national and international data privacy laws is a daunting task. Legislation struggles to keep pace with rapid technological advancements, leading to a lack of consistency and clarity in data protection regulations. This regulatory fragmentation complicates compliance efforts for organizations operating across borders.

The role of a United Nations (UN)-led global data privacy authority emerges as a potential solution, offering a framework for international cooperation, harmonized standards, and ethical guidelines. In subsequent sections, we will delve deeper into these challenges and examine how a UN-led global data privacy authority can address them, paving the way for a more secure and harmonized data governance framework in the digital age.[28]

3.2 Data Collection, Processing, and Trading Trends

The rapid proliferation of technology and digitalization has fundamentally reshaped the landscape of

[25] PAGOROPOULOS, A.; PIGOSSO, D. C.; MCALOONE, T. C. The emergent role of digital technologies in the Circular Economy: a review. *Procedia CIRP*, 2017.

[26] ZHU, Y.; ZHONG, N.; XIONG, Y. Data explosion, data nature and dataology. *Springer Link*, p. 147-158, 2009.

[27] BERGHEL, H. The equifax hack revisited and repurposed. *Computer*, v. 53, n. 5, p. 85, 2020.

[28] HERT, Paul de; PAPAKONSTANTINOU, Vagelis. Three Scenarios for International Governance of Data Priv-acy: towards an International Data Privacy Organ-ization, Preferably a UN Agency?. *A Journal of Law and Policy for the Information Society,* p. 271, 2013.

data collection, processing, and trading. In this era, data is often referred to as the new currency, and the trends in its collection, processing, and trading are at the forefront of discussions on data privacy and security. Data collection has become pervasive and continuous in the digital age. The proliferation of connected devices, from smartphones and smartwatches to Internet of Things (IoT) sensors, means that individuals are constantly generating data. This data encompasses a wide range of information, including location data, browsing habits, social media interactions, and health metrics. Social media platforms and online services play a central role in data collection. Users willingly share personal details, preferences, and behaviours on these platforms, often unaware of the extent to which their data is being harvested. In addition, e-commerce sites track shopping patterns and user preferences, contributing to the wealth of data available for analysis. Furthermore, data collection extends to offline activities through technologies like facial recognition and biometric data capture, further blurring the lines between the physical and digital realms.

The digital age has witnessed a revolution in data processing capabilities. Artificial intelligence (AI), machine learning, and advanced analytics have empowered organizations to extract valuable insights from vast datasets. These technologies enable real-time analysis, predictive modeling, and the automation of decision-making processes. For instance, in the healthcare sector, AI algorithms can analyze medical images to detect diseases or predict patient outcomes. In finance, predictive analytics can identify fraudulent transactions by recognizing patterns in transaction data. In marketing, machine learning algorithms power recommendation engines that tailor product suggestions to individual user preferences. This data processing prowess has the potential to enhance various aspects of our lives but also raises concerns about the responsible and ethical use of personal data. Ensuring that data processing respects privacy rights and maintains data security is crucial in this context.[29]

Data has emerged as a valuable commodity in the digital economy. Data brokers, advertisers, and technology companies engage in data trading to monetize the information they collect. User profiles are created, enriched, and sold to interested parties. This data trading ecosystem is complex and opaque. Users often have little control over how their data is used and may not be aware of the extent to which their information is being bought and sold. Advertisers leverage this data to deliver highly targeted ads, while companies use it to gain competitive advantages. The commodification of personal data raises ethical concerns. It prompts discussions about transparency, user consent, and the need for regulations that protect individuals from potential abuses of their data.[30]

3.3 Challenges to Data Privacy and Security

As data collection, processing, and trading trends evolve, they bring forth a host of challenges to data privacy and security that demand careful consideration and action. The interconnected digital world is vulnerable to a myriad of cybersecurity threats. Cybercriminals and hackers continually exploit vulnerabilities in networks, software, and hardware to gain unauthorized access to sensitive data. Large-scale data breaches have become distressingly common, exposing personal information, financial records, and even classified government data. These breaches result in financial losses, damage to reputation, and the potential for identity theft and fraud. Protecting data from cyber threats has become a top priority for individuals, organizations, and governments.

Some examples of the global data breach issues that illustrate these challenges are:

a. The CAM data breach in March 2020 exposed over 10 billion records of adult video streaming website users, including their full names, email addresses, sexual orientation, chat transcripts, payment logs, and IP addresses1. This breach exposed users to the risk of blackmail, extortion, and harassment by cybercriminals who could exploit their sensitive and personal information.[31]

b. The Yahoo data breach in 2017 affected 3 billion user accounts, compromising their security questions and answers, which could be used to access other online accounts2. This breach eroded user trust and

[29] ZHAO, J; MORTIER, R; CROWCROFT, J; WANG, L. *Privacy-preserving machine learning based data analytics on edge*. 2018.

[30] ESTADELLA-YUSTE, Olga. Transborder data flows, and the sources of public international law. *North Carolina Journal of International Law*, v. 16, n. 2, 1991.

[31] MURTHY, M. S. Data protection law and policy in the USA: an overview. *Indian JL & Legal Research,* n. 3, 2022.

confidence in Yahoo's ability to protect their data and resulted in a significant reduction in Yahoo's sale price to Verizon.[32]

c. The Aadhaar data breach in 2018 revealed that the personal details of more than a billion citizens in India stored in the world's largest biometric database could be bought online3. This breach exposed users to the risk of identity theft, fraud, and misuse of their biometric data by unauthorized parties.[33]

d. The Accellion data breach in 2021 affected hundreds of organizations that used Accellion's file transfer service to share sensitive data. This breach compromised the data of millions of individuals, including their health records, financial information, and personal details. Some of the victims included the Reserve Bank of New Zealand, the Australian Securities and Investments Commission, the University of Colorado, and Kroger.[34]

Lack of Privacy Awareness: Many individuals are unaware of the extent to which their data is collected and how it is used. Complex privacy policies and consent forms laden with legal jargon often hinder informed decision-making. Users may unwittingly agree to the collection and sharing of their data without fully comprehending the consequences.

This lack of privacy awareness erodes trust and makes it challenging for individuals to exercise their right to control their personal information. Education and user-friendly privacy practices are needed to address this issue.

Some examples of the lack of privacy awareness that illustrate this issue are:

a. The Facebook-Cambridge Analytica scandal in 2018 revealed that Facebook had allowed a third-party app developer to harvest the data of millions of users without their consent or knowledge. This data was then used by Cambridge Analytica to influence political campaigns and elections around the world. This scandal sparked public outrage and scrutiny over Facebook's privacy practices and policies.[35]

b. The Google Street View controversy in 2010 exposed that Google had collected personal data from unencrypted Wi-Fi networks while taking pictures for its Street View service. This data included emails, passwords, browsing history, and other sensitive information. Google claimed that this was an inadvertent mistake and that it did not use or retain the data. However, this incident raised concerns over Google's respect for user privacy and compliance with data protection laws.[36]

c. The Clearview AI controversy in 2020 revealed that Clearview AI had scraped billions of images from social media platforms and websites to create a facial recognition database that it sold to law enforcement agencies. This database was used to identify suspects and persons of interest without their consent or awareness. This controversy raised ethical questions over Clearview AI's use of public data for private profit and its potential impact on civil liberties and human rights.[37]

Legislative Gaps: National and international data privacy laws struggle to keep pace with rapid technological advancements. This results in a fragmented regulatory landscape, with varying standards and levels of protection across different regions. The lack of consistency and clarity in data protection regulations poses challenges for multinational corporations operating across borders. Complying with a patchwork of laws can be complex and costly, creating the need for greater harmonization and global cooperation in data governance.

Some examples of the legislative gaps that illustrate this issue are:

a. The EU-US Privacy Shield framework was an agreement between the EU and the US that aimed to facilitate the transfer of personal data between the two regions by providing a mechanism for US companies to demonstrate GDPR compliance. However, in July 2020, the European Court of Justice invalidated the Privacy Shield, citing concerns about US government survei-

[32] WHITLER, K. A.; FARRIS, P. W. The impact of cyber-attacks on brand image: why proactive marketing expertise is needed for managing data breaches. *Journal of Advertising Research*, v. 57, n. 1, p. 3-9, 2017.

[33] TYAGI, A. K.; REKHA, G.; SREENATH, N. Is your privacy safe with Aadhaar?: an open discussion'. *IEEE,* Solan, p. 318-323, 2018.

[34] KOFF, E. *NSW Accellion Data Breach*. 2020.

[35] CONFESSORE, Nicholas. *Cambridge Analytica and Facebook*: the scandal and the Fallout So Far. 2018. Available in: https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.

[36] HALLIDAY, Josh. Google faces new Street View data controversy. *The Guardian*, 2012.

[37] REZENDE, I. N. Facial recognition in police hands: assessing the 'Clearview case' from a European perspective. *New Journal of European Criminal Law*, p. 375-89, 2020.

llance practices. This ruling created uncertainty and disruption for thousands of businesses that relied on the Privacy Shield for transatlantic data flows.[38]

b. The GDPR is the most comprehensive and influential data protection law in the world. It applies to the EU and the EEA, as well as to any entity that processes the personal data of individuals in these regions. However, the GDPR also faces challenges in its implementation and enforcement, such as the lack of resources and coordination among national data protection authorities, the inconsistency and divergence in national interpretations and applications of the GDPR, and the difficulty in imposing effective sanctions and remedies for cross-border violations.

c. The PIPL is the first comprehensive data protection law in China. It applies to any entity that processes the personal information of individuals in China or provides products or services to individuals in China. However, the PIPL also faces challenges in its alignment and compatibility with other data protection regimes, such as the GDPR. For example, the PIPL has different definitions and categories of personal information, different legal bases and conditions for data processing, different requirements and exemptions for cross-border data transfers, and different rights and obligations for data subjects and processors.[39]

Ethical Concerns: The use of data for profiling, surveillance, and targeted advertising raises ethical questions. It highlights the importance of ethical guidelines and principles in data handling, especially when data is used to make decisions that can profoundly affect individuals' lives, such as in lending, employment, or healthcare.

Some examples of the ethical concerns that illustrate this issue are:

a. The use of facial recognition technology for law enforcement purposes has been criticized for its potential to violate privacy, civil liberties, and human rights. Facial recognition technology can be used to track, monitor, and identify individuals without their consent or knowledge. It can also be prone to errors and biases, resulting in false positives, misidentification, and discrimination.[40]

b. The use of social media data for political campaigning and manipulation has been condemned for its potential to undermine democracy, influence public opinion, and spread misinformation. Social media data can be used to profile voters based on their preferences, behaviors, and emotions. It can also be used to target them with personalized messages, ads, and content that can sway their voting decisions.[41]

c. The use of health data for research and innovation has been praised for its potential to improve health outcomes, prevent diseases, and discover new treatments. Health data can be used to analyze patterns, trends, and correlations among various health factors. It can also be used to develop personalized medicine, diagnostics, and therapies. However, the use of health data also raises ethical issues such as consent, confidentiality, ownership, access, and security. Health data is sensitive and personal information that can reveal intimate details about individuals' physical and mental health. It can also be subject to misuse, abuse, and exploitation by unauthorized parties.[42]

In conclusion, the digital age has ushered in a new era of data collection, processing, and trading, bringing with it both opportunities and challenges. The responsible handling of data, safeguarding data privacy and security, and ensuring that individuals have control over their personal information are pressing issues in this digital landscape. The role of a United Nations (UN)-led global data privacy authority becomes increasingly relevant in addressing these challenges and fostering a more secure and harmonized data governance framework on a global scale.

[38] EUROPEAN UNION. Department of Commerce and the European Commission, UK Government, and Swiss Federal Administration. *Privacy Shield Framework*. Available in: https://www.privacyshield.gov/ps/eu-us-framework.

[39] CALZADA, I. Citizens data privacy in China: the state of the art of the Personal Information Protection Law (PIPL) *Smart Cities,* p. 1129-50, 2022.

[40] HIROSE, M. Privacy in public spaces: the reasonable expectation of privacy against the dragnet use of facial recognition technology. *Conn. L. Rev*, 2016.

[41] DIMITROVA, D. V.; MATTHES, J. Social media in political campaigning around the world: theoretical and methodological challenges. *Journalism & mass communication quarterly*, v. 95, n. 2, p. 333-42, June 2018.

[42] ABOUELMEHDI, K.; BENI-HESSANE, A.; KHALOUFI, H. Big healthcare data: preserving security and privacy. *Journal of big data*, p. 1-8, 2018.

4 Global Data Privacy Landscape

4.1 Varied Data Privacy Laws Across Jurisdictions

In today's interconnected world, one of the most prominent challenges in the realm of data privacy is the significant variation in data protection laws across different jurisdictions. This diversity arises from the complex interplay of historical, cultural, and legal factors, resulting in a patchwork of regulations that govern the collection, processing, and sharing of personal data. The implications of this variance are far-reaching, affecting individuals, corporations, and governments alike.[43]

Data privacy laws can differ dramatically from one jurisdiction to another. For instance, the European Union's General Data Protection Regulation (GDPR) imposes stringent requirements on organizations, emphasizing principles such as data minimization, purpose limitation, and the right to be forgotten. Meanwhile, in the United States, the privacy landscape is fragmented, with a mix of federal and state laws, as well as industry-specific regulations. These variations can pose substantial compliance challenges for multinational corporations that operate in multiple regions, forcing them to navigate a complex web of legal requirements.[44]

4.2 The Need for Global Regulatory Solutions

Given the challenges posed by varied data privacy laws, there is a growing recognition of the need for global regulatory solutions to address these complexities. A harmonized and consistent approach to data privacy can offer numerous benefits:

Streamlined Compliance: Global regulatory standards can simplify compliance efforts for organizations operating across multiple jurisdictions. A unified framework reduces the need for tailored compliance programs for each region, making it more efficient and cost-effective to protect individuals' privacy.

Enhanced Data Flow: A standardized approach to data privacy facilitates the seamless flow of data across borders. This is crucial for global business operations, international research collaboration, and the development of emerging technologies such as cloud computing and AI.

Improved Privacy Rights: A global regulatory solution can strengthen individuals' privacy rights by establishing consistent and robust protections regardless of their location. This ensures that individuals have a uniform level of control over their personal data, regardless of where it is processed or stored.

Effective Cross-Border Cooperation: International law enforcement and cooperation in addressing cybercrimes and data breaches are enhanced when there is clarity and consistency in data privacy regulations. This fosters collaboration in pursuing cybercriminals and ensuring justice is served.

The variation in data privacy laws across jurisdictions presents significant challenges for individuals, corporations, and governments. While harmonizing these regulations is a complex undertaking, there is a growing consensus on the need for global regulatory solutions that strike a balance between protecting privacy and enabling innovation in our increasingly interconnected world. Such solutions hold the promise of fostering a more secure, efficient, and equitable data privacy landscape on a global scale.[45]

5 Proposal for a United Nations Data Privacy Body

The scope and scale of the digital ecosystem have grown exponentially in recent years, generating a vast amount of data on individuals and organizations. This data, often termed as the "new gold," has become a critical resource for economic and social development. However, concerns about data privacy and protection have also risen. With the emergence of new technologies such as artificial intelligence and the Internet of Things, challenges related to data privacy have become

[43] SVANTESSON, D. Enforcing privacy across different jurisdictions. Enforcing privacy: regulatory, legal and technological approaches. *Springer,* p. 195-222, 2016. Available in: https://link.springer.com/chapter/10.1007/978-3-319-25047-2_9.

[44] AUSLOOS, J. The 'right to be forgotten': worth remembering?. *Computer law & security review*, v. 28, n. 2, p. 143-52, 2012.

[45] GREENLEAF, Graham. A world data privacy treaty? "globalization" and "modernization" of Council of Europe Convention 108. *In*: WITZLEB, N. *et al.* (ed.). *Emerging challenges in privacy law*: comparative perspectives. Cambridge: Cambridge University Press, 2014.

increasingly complex and global in nature.[46] This proposal aims to address these challenges by advocating for the establishment of a United Nations Data Privacy Body, in alignment with the World Intellectual Property Organization (WIPO), to provide a comprehensive and harmonized framework for data privacy regulations worldwide.

5.1 The Feasibility of Establishing a Global Data Privacy Body

The establishment of a global data privacy body, such as a United Nations (UN) agency dedicated to data privacy, is a concept that is gaining momentum in the digital age. Its feasibility rests on several key factors. Firstly, the increasing interconnectedness of our world highlights the need for a unified approach to data privacy that transcends borders. Secondly, the growing concerns about data breaches, privacy violations, and surveillance underscore the urgency of addressing these issues at an international level.[47] The success of existing UN agencies, such as the World Health Organization (WHO) and the International Monetary Fund (IMF), demonstrates the capacity of the UN to effectively manage global challenges.

5.2 Role and Scope of the Proposed UN Agency

Furthermore, the need for a United Nations data privacy body is evident due to the growing concerns over the lack of comprehensive international regulations on data privacy. As highlighted by the World Intellectual Property Organization (WIPO), there is currently no global framework that adequately addresses the complex challenges of data protection. This has resulted in various countries and regions implementing their own data privacy laws, leading to a fragmented regulatory landscape that hinders cross-border data transfers and creates confusion for businesses.[48] To overcome these obstacles, a United Nations data privacy body would serve as a central authority responsible for developing consistent and harmonized global standards and guidelines on data protection, thereby promoting the effective and secure exchange of data on an international level. Considering the escalating data privacy violations and breaches, the establishment of a United Nations Data Privacy Body, following the model of the World Intellectual Property Organization (WIPO), is imperative. Firstly, an international body solely dedicated to addressing data privacy concerns would facilitate the development of standardized regulations and enforcement mechanisms across nations. Importantly, this body would actively promote and streamline international cooperation in handling data privacy issues. Secondly, by providing a platform for knowledge-sharing and capacity-building among nations, this body could empower countries to better protect their citizens' personal information in an increasingly digitalized world. Lastly, such an organization would also play a pivotal role in fostering global information exchange while ensuring the preservation of individual privacy rights.[49] Overall, the establishment of a United Nations Data Privacy Body will effectively address growing concerns over data privacy violations and breaches while promoting global cooperation and knowledge-sharing.

5.3 Leveraging UN Expertise and Resources

The proposed United Nations Data Privacy Body would play a crucial role in protecting individuals' privacy rights in the digital age. Its functions would encompass monitoring the implementation and enforcement of data privacy regulations globally, facilitating international cooperation on data protection issues, and developing best practices and standards to ensure the responsible handling of personal data. As noted by Voss, W. Gregory, such a body would serve as a central authority for addressing cross-border data privacy concerns and harmonizing data protection laws across different jurisdictions.[50] Additionally, it would provide a platform for public engagement and education to raise awareness about the importance of privacy in the digital era. In order to effectively address the challenges associated with data privacy in the digital era, it is imperative to establish global data privacy standards and guidelines.

[46] YILMA, Kinfe. *Privacy and the role of International Law in the digital age*. 2023.

[47] GREENLEAF, Graham. Data protection in a globalized network. *In*: BROWN, I. (ed). *Research handbook on governance of the internet*. Cheltenham: Edward Elgar, 2012.

[48] AARONSON, Susan Ariel. Data is different, and that's why the world needs a new approach to governing cross-border data flows. *Digital Policy, Regulation and Governance*, v. 21, n. 5, p. 441-460, 2019.

[49] YILMA, Kinfe. *Privacy and the role of International law in the digital age*. 2023.

[50] VOSS, W. Gregory. Cross-border data flows, the GDPR, and data governance. *Wash. Int'l LJ*, v. 29, p. 485, 2019.

These standards and guidelines would serve as a framework for countries to develop and enforce their own data privacy regulations. Moreover, a unified approach would enhance cross-border data protection and empower individuals to exercise control over their personal information. A global data privacy body similar to the World Intellectual Property Organization (WIPO) under the United Nations could ensure harmonization of standards and provide a platform for international cooperation on data privacy issues. Monitoring and enforcing compliance with data privacy regulations is crucial to ensure the protection of individuals' personal information.[51] A United Nations Data Privacy Body (UNDPB) could play a vital role in this process, overseeing international data transfers and enforcing regulations in line with the World Intellectual Property Organization (WIPO). By establishing a UNDPB, member states would be able to collaborate, share best practices, and implement accountability mechanisms to combat emerging privacy challenges. Such efforts would foster a global standard for data privacy protection, strengthening individuals' trust in the digital economy. To achieve a comprehensive and effective data privacy framework, it is crucial to facilitate international cooperation and information sharing on data privacy issues.[52] With the exponential growth of cross-border data flows and increasing concerns over data protection, collaboration among nations becomes imperative. By creating a specialized United Nations Data Privacy Body in lines with WIPO, countries can come together to exchange best practices, harmonize policies, and establish common regulatory standards. This global cooperation would ensure the consistent protection of individuals' data regardless of their geographical location, thereby fostering trust and maintaining the integrity of the digital economy. The establishment of a United Nations Data Privacy Body that aligns with the World Intellectual Property Organization (WIPO) is crucial in this digital era of heightened privacy concerns. The unprecedented growth of technology has exponentially increased the risk of data breaches and privacy violations. A dedicated UN body would be responsible for formulating international policies that protect individual privacy rights, promote data security, and regulate the activities of technology companies. Such a body would ensure consistency, harmonization, and global cooperation in addressing the complexities of data privacy.

5.4 Potential Benefits of the UN Data Privacy Agency

The creation of a UN data privacy agency offers several potential benefits. Firstly, it would promote the harmonization of data protection laws, reducing compliance burdens for organizations operating internationally. Secondly, it would enhance individuals' privacy rights by ensuring consistent and robust data protection regardless of their location. Thirdly, the agency would foster international cooperation in addressing cybercrimes, data breaches, and privacy violations, strengthening global cybersecurity efforts. Finally, it would contribute to the development of ethical guidelines for emerging technologies like AI and biotechnology, safeguarding human rights and dignity in the digital age.[53]

The feasibility of establishing a global data privacy agency under the auspices of the United Nations is rooted in the pressing need for a unified approach to data privacy, the urgency of addressing global data privacy challenges, and the UN's track record in managing international issues. Such an agency holds the potential to harmonize regulations, protect individuals' privacy, enhance cybersecurity, and provide ethical guidance, ultimately fostering a more secure and equitable data privacy landscape on a global scale.

6 Comparison to WIPO's Role in Intellectual Property Rights

In alignment with WIPO, the establishment of a United Nations Data Privacy Body would contribute to strengthening and harmonizing international efforts to safeguard individuals' privacy in the digital age. The World Intellectual Property Organization (WIPO) has been successful in developing international frameworks

[51] GREENLEAF, Graham. Global data privacy laws 2019: new eras for International Standards. *Privacy Laws & Business International Report,* p. 19-20, 2019. Available in: https://ssrn.com/abstract=3384012.

[52] GREENLEAF, Graham. Data protection in a globalized network. *In*: BROWN, I. (ed). *Research handbook on governance of the internet*. Cheltenham: Edward Elgar, 2012.

[53] UN GLOBAL PULSE. *UN global pulse principles on data protection and privacy*. Available in: https://www.unglobalpulse.org/policy/ungp-principles-on-data-privacy-and-protection/.

and standards for intellectual property protection.[54] Similarly, a UN Data Privacy Body could provide a forum for member states to develop and promote common principles, guidelines, and standards for data privacy, ensuring a comprehensive and consistent approach globally. This alignment with WIPO would enhance cooperation and collaboration among nations, facilitating the implementation of effective data privacy regulations and providing a solid foundation for cross-border data protection. Furthermore, the issue of data privacy shares several similarities with intellectual property rights. Both concepts involve the protection of valuable assets and the recognition of ownership rights. Just as intellectual property rights safeguard innovative ideas, data privacy ensures the protection of personal information. Similar to how infringements on intellectual property rights can lead to financial losses and reputational damage for creators, violations of data privacy can result in identity theft and privacy breaches. These similarities emphasize the need for a dedicated international body to address data privacy concerns in a manner consistent with existing frameworks for intellectual property rights.[55]

6.1 Lessons from WIPO's Success: Parallels in International Data Governance

The World Intellectual Property Organization (WIPO) stands as a testament to the effectiveness of international collaboration and harmonization of laws in protecting intellectual property rights (IPR) globally. WIPO, established in 1967 as a specialized agency of the United Nations, has played a pivotal role in shaping a consistent framework for IP protection across the world. By examining the history of WIPO conventions and its accomplishments, valuable lessons can be drawn for addressing data protection rights and regulating cross-border issues in data privacy.[56]

WIPO's success story is underpinned by the convergence of nations around common principles and standards for IPR. It's worth noting that the journey began with the Berne Convention for the Protection of Literary and Artistic Works in 1886, which aimed to establish a universal copyright framework. This convention laid the foundation for international collaboration in the field of IP. Subsequently, the Paris Convention for the Protection of Industrial Property in 1883 marked a significant milestone in harmonizing the protection of industrial property. In a manner parallel to WIPO's history, addressing data protection rights on a global scale requires international collaboration. The establishment of a UN-led agency dedicated to data protection rights could serve as a catalyst for this. Member states would work together to develop treaties and agreements that set common standards for data protection, ensuring that individuals' data privacy rights are consistently respected across borders. Just as the Berne Convention harmonized copyright protection, similar international agreements could harmonize data protection laws and regulations. These agreements would provide a unified framework for data privacy, making compliance with consistent standards more manageable for organizations worldwide.

Capacity building and education have been pivotal in WIPO's success. The organization has offered training, technical assistance, and support to help member states strengthen their IP systems. This has been particularly important for developing countries looking to better understand and implement IP laws and regulations. Similarly, a UN-led data protection agency could provide capacity-building programs and technical assistance to bolster member states' data protection systems. This training would encompass understanding data protection laws, implementing cybersecurity measures, and best practices in data handling.

Effective dispute resolution mechanisms, such as WIPO's Arbitration and Mediation Center, are vital for maintaining a fair and predictable environment for IP rights holders. Similarly, establishing a mechanism for resolving cross-border data privacy disputes would be crucial. This dedicated body would offer efficient and impartial dispute resolution services to address conflicts related to data privacy.

Moreover, public awareness campaigns have been a hallmark of WIPO's efforts to educate the public about the importance of IP rights. These campaigns foster respect for IP rights and encourage innovation and creativity. Similarly, promoting public awareness about data protection rights and privacy would be paramount.

[54] BOYLE J. A manifesto on WIPO and the future of intellectual property. *Duke L. & Tech. Rev.,* 2004.

[55] BOYLE, J. A manifesto on WIPO and the future of intellectual property. *Duke L. & Tech. Rev.,* 2004.

[56] WIPO Convention. 1967. Available in: https://www.wipo.int/portal/en/index.html.

It would empower individuals to understand and assert their data protection rights, fostering a more privacy--conscious society.

The historical success of WIPO in the realm of intellectual property rights, shaped by international collaboration and harmonization of laws, provides valuable lessons for establishing common principles for data protection rights and regulating cross-border issues in data privacy. By leveraging these lessons, a UN-led data protection agency could pave the way for a more secure and harmonized data governance framework on a global scale, much like the achievements of WIPO in the field of intellectual property.[57]

6.2 Why WIPO's role model taken in the present case is based on following factors:

a. Global Agreements: WIPO has successfully negotiated and administered international treaties and agreements, such as the Paris Convention for the Protection of Industrial Property and the Berne Convention for the Protection of Literary and Artistic Works. These agreements have set global standards for the protection of intellectual property.

b. Promotion of Innovation: WIPO's initiatives aim to balance the interests of creators and innovators with the broader goal of promoting innovation and creativity worldwide. This approach has been seen as a model for fostering innovation within a framework of legal protection.

c. Capacity Building: WIPO provides technical assistance and capacity-building programs to help countries, especially developing nations, establish and strengthen their intellectual property systems. This support enhances access to global markets and encourages innovation.

d. Dispute Resolution: WIPO's Arbitration and Mediation Center is a model for resolving intellectual property disputes through alternative dispute resolution mechanisms, offering an efficient and cost-effective means of settling conflicts.

While each UN organization has its unique role and contributions, WIPO's success in its specific field has made it a role model for international cooperation in intellectual property rights and innovation.

7 Conclusion

7.1 Summarizing Key Findings and Insights

A. Enhanced protection of individuals' privacy rights globally Furthermore, the establishment of a United Nations Data Privacy Body aligned with WIPO would create an opportunity for enhanced protection of individuals' privacy rights on a global scale. Currently, there is a lack of a comprehensive international framework that adequately addresses privacy concerns in the digital age. As stated by Kuner, the existing patchwork of national legislations and regional agreements fails to effectively address the challenges posed by cross-border data flows and the increasing power of big tech corporations. Such a body would provide a much-needed platform for harmonizing privacy standards and facilitating international cooperation in this field. [58]

B. Promotion of trust and confidence in the digital economy the promotion of trust and confidence in the digital economy is a crucial aspect to consider, as it is directly linked to the success and growth of online industries. In this era of extensive data sharing and dependence on technology, individuals and businesses are increasingly concerned about the protection of their data and privacy. Establishing a specialized United Nations Data Privacy Body, in line with the World Intellectual Property Organization (WIPO), can address these concerns by providing a global framework and guidelines for data protection.[59]

C. Facilitation of cross-border data flows while ensuring privacy safeguards Furthermore, the establishment of a United Nations Data Privacy Body in line with the World Intellectual Property Organization

[57] MOSSINGHOFF, G. J.; OMAN, R. The World Intellectual Property Organization: a United Nations success story. *World Affs*, 1997.

[58] KUNER, C. International Organizations and the EU general data protection regulation: exploring the interaction between EU law and international law. *International Organizations Law Review*, v. 16, n. 1, p 158-191, 2019. Available in: https://doi.org/10.1163/15723747-2019008.

[59] A World That Counts: Mobilizing the Data Revolution for Sustainable Development, Report Prepared at the Request of the UN Secretary General by the Independent Expert Advisory Group on a Data Revolution for Sustainable Development, November, 2014.

(WIPO) could effectively address the facilitation of cross-border data flows while maintaining privacy safeguards. The increasing globalization and digitalization of information have necessitated the need for harmonized international measures to ensure data protection.[60] This proposed body would serve as a global platform for countries to collaborate on developing standardized legal frameworks and practices for cross-border data transfers, striking a balance between data privacy concerns and the need for seamless data flow. The creation of a United Nations (UN) Data Privacy Body is crucial in addressing the challenges brought about by the increasing digitalization and global exchange of personal information. The World Intellectual Property Organization (WIPO) has played a central role in standardizing intellectual property rights at the international level. However, in the sphere of data privacy, there is a clear gap in international governance. Establishing a UN Data Privacy Body would fill this void by ensuring the protection of individuals' privacy rights in the digital age. [61]

7.2 Advocating for the UN's Role in International Data Governance

The establishment of a United Nations Data Privacy Body aligned with WIPO poses several challenges, but potential solutions can be identified. One challenge concerns the integration of diverse national laws and regulations, varying in scope and content, into a unified framework. However, this could be addressed through the adoption of a comparative approach, considering the best practices and principles from different jurisdictions.[62] Another challenge is the harmonization of international standards and norms, which may require extensive negotiations and consensus-building among member states. Nonetheless, with a commitment to multilateral cooperation, this challenge can be surmounted. Lastly, the implementation and enforcement of data privacy laws demand effective mechanisms for monitoring compliance and resolving disputes. Utilizing innovative technologies, such as blockchain and artificial intelligence, can enhance transparency, accountability, and efficiency in this regard.[63]

8 Recommendations and Future Directions

1. Concrete Recommendations for UN Action

Balancing privacy rights with legitimate interests of businesses and governments. In the context of rapidly advancing technology and globalization, there is an increasing need to navigate the delicate balance between privacy rights and the legitimate interests of businesses and governments. While individuals have the right to protect their personal information, businesses and governments have valid reasons to collect and utilize this data for various purposes, such as national security and economic development. However, striking the right balance can be challenging, as it requires addressing the concerns of both individuals and the entities that rely on this data.

2. Addressing differing cultural and legal perspectives on data privacy

Ensuring data privacy in today's globalized world is complex due to the existence of differing cultural and legal perspectives. Different countries have varying regulations and cultural norms surrounding data privacy, which can create challenges when sharing and protecting personal information across borders. For instance, some countries emphasize individual privacy rights, while others prioritize national security or economic interests.

3. Addressing these differences requires a unified international approach.

The establishment of a United Nations Data Privacy Body aligned with the World Intellectual Property Organization (WIPO) would enable the creation of global standards and guidelines to harmonize and respect cul-

[60] MISHRA, Neha. Data localization laws in a digital world: data protection or data protectionism?. *The Public Sphere,* 2015.

[61] BYGRAVE, Lee A. Privacy protection in a global context–a comparative overview. *Scandinavian Studies in Law*, v. 47, p. 319-348, 2004.

[62] SULLIVAN, Clare. EU GDPR or APEC CBPR? a comparative analysis of the approach of the EU and APEC to cross border data transfers and protection of personal data in the IoT era. *Computer law & security review*, v. 35, n. 4, p. 380-397, 2019.

[63] BOSRI, Rabeya; RAHMAN, Mohammad Shahriar; BHUIYAN, Md Zakirul Alam; OMAR, Abdullah Al. Integrating blockchain with artificial intelligence for privacy-preserving recommender systems. *IEEE Transactions on Network Science and Engineering,* v. 8, n. 2, p. 1009-1018, 2020.

tural diversity while protecting individuals' data privacy rights.[64]

4. Establishing effective mechanisms for resolving disputes and enforcing regulations.

Dispute resolution and enforcement of regulations are crucial aspects in the establishment of an effective United Nations data privacy body. Ensuring that mechanisms are in place to address disputes promptly and efficiently is imperative to maintain accountability and transparency in data privacy matters. Additionally, the enforcement of regulations is vital to safeguard individuals' privacy rights and to hold organizations accountable for any violations. A dedicated dispute resolution mechanism could contribute to resolving conflicts between countries or between individuals and organizations, promoting a standardized and fair approach to resolving disputes. The establishment of a United Nations Data Privacy Body in line with the World Intellectual Property Organization (WIPO) is crucial in the digital age where personal information is increasingly vulnerable to misuse and exploitation. This body would serve as a global authority responsible for setting and implementing data privacy regulations, ensuring transparency, and safeguarding individuals' rights in the digital realm. By aligning with WIPO's principles, which have successfully regulated intellectual property on an international scale, this new body can effectively tackle the emerging challenges of data privacy in a globalized and interconnected world.

The Road Ahead: Implementing the Proposed Agency

In conclusion, the establishment of a dedicated United Nations Data Privacy Body aligned with the World Intellectual Property Organization (WIPO) is imperative to address the growing challenges of global data protection. The existing mechanisms within the UN framework, including the General Assembly and Human Rights Council, fall short in effectively coordinating and enforcing data privacy policies on an international scale. By incorporating the expertise and mandates of WIPO, this proposed body can harmonize data protection laws, facilitate international cooperation, and uphold the fundamental right to privacy in the digital age. A United Nations Data Privacy Body, similar to the World Intellectual Property Organization (WIPO), has the potential to significantly impact and benefit the protection of data privacy worldwide. Firstly, it could establish global data privacy standards and regulations, ensuring consistency across countries and bridging the gaps in existing legal frameworks. Additionally, this body could facilitate international cooperation and collaboration in addressing data privacy concerns, promoting harmonization, and fostering trust among nations. The presence of such a body could also enhance transparency, accountability, and enforcement mechanisms, ultimately leading to greater data protection and privacy for individuals and organizations.

[64] ABBOTT, Kenneth; DUNCAN, Hard Snidal. *Soft Law in International Governance*. International Organization, 2000. p. 421.

References

AARONSON, Susan Ariel. Data is different, and that's why the world needs a new approach to governing cross-border data flows. *Digital Policy, Regulation and Governance,* v. 21, n. 5, p. 441-460, 2019.

ABBOTT, Kenneth; DUNCAN, Hard Snidal. *Soft Law in International Governance*. International Organization, 2000.

ABOUELMEHDI, K.; BENI-HESSANE, A.; KHALOUFI, H. Big healthcare data: preserving security and privacy. *Journal of big data*, p. 1-8, 2018.

AUSLOOS, J. The 'right to be forgotten': worth remembering? *Computer law & security review*, v. 28, n. 2, p. 143-52, 2012.

A WORLD that counts: mobilizing the data revolution for sustainable development, report prepared at the request of the UN Secretary General by the Independent Expert Advisory Group on a data revolution for sustainable development. 2014.

BERGHEL, H. The equifax hack revisited and repurposed. *Computer*, v. 53, n. 5, p. 85, 2020.

BOSRI, Rabeya; RAHMAN, Mohammad Shahriar; BHUIYAN, Md Zakirul Alam; OMAR, Abdullah Al. Integrating blockchain with artificial intelligence for privacy-preserving recommender systems. *IEEE Transactions on Network Science and Engineering,* v. 8, n. 2, p. 1009-1018, 2020.

BOYLE, J. A manifesto on WIPO and the Future of Intellectual Property. *Duke L. & Tech. Rev.,* 2004.

BYGRAVE, Lee A. Privacy protection in a global context–a comparative overview. *Scandinavian Studies in Law*, v. 47, p. 319-348, 2004.

CALZADA, I. Citizens data privacy in China: the state of the art of the Personal Information Protection Law (PIPL). *Smart Cities,* p. 1129-50, 2022.

CASALINI, F.; GONZÁLEZ, J. L. *Trade and cross-border data flows*. 2019.

COMPAGNUCCI, M. Corrales; ABOY, M.; MINSSEN, T. *Cross-border transfers of personal data after Schrems II*: supplementary measures and new standard contractual clauses (SCCs). 2021.

CONFESSORE, Nicholas. *Cambridge Analytica and Facebook*: the scandal and the Fallout So Far. 2018. Available in: https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.

CORTEZ, E. K. (ed.). Data protection around the world: privacy laws in action. *Springer Nature*, 20 Nov. 2020.

HERT, Paul de; PAPAKONSTANTINOU, Vagelis. Three Scenarios for International Governance of Data Priv-acy: towards an International Data Privacy Organization, Preferably a UN Agency?. *A Journal of Law and Policy for the Information Society*, p. 271, 2013.

DIMITROVA, D. V.; MATTHES, J. Social media in political campaigning around the world: theoretical and methodological challenges. *Journalism & mass communication quarterly*, v. 95, n. 2, p. 333-42, June 2018.

ESTADELLA-YUSTE, Olga. TransborderL data flows, and the sources of public international law. *North Carolina Journal of International Law*, v. 16, n. 2, 1991.

EUROPEAN COMMISSION. *Data protection*: European Commission adopts new adequacy decision for safe and trusted EU-US data flows. 2023. Available in: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721.

EUROPEAN COMMISSION. *Questions & answers*: EU-US data privacy framework. 2023. Available in: https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_3752.

EUROPEAN UNION. Court of Justice of the European Union. *Data protection commissioner v Facebook Ireland and Maximillian Schrems C-311/18*. 2020.

EUROPEAN UNION. Department of Commerce and the European Commission, UK Government, and Swiss Federal Administration. *Privacy Shield Framework*. Available in: https://www.privacyshield.gov/ps/eu-us-framework.

GREENLEAF, Graham. A world data privacy treaty? "globalization" and "modernization" of Council of Europe Convention 108. *In*: WITZLEB, N. *et al.* (ed.). *Emerging challenges in privacy law*: comparative perspectives. Cambridge: Cambridge University Press, 2014.

GREENLEAF, Graham. Data protection in a globalized network. *In*: BROWN, I. (ed). *Research handbook on governance of the internet*. Cheltenham: Edward Elgar, 2012.

GREENLEAF, Graham. Global data privacy laws 2019: new eras for International Standards. *Privacy Laws & Business International Report,* p. 19-20, 2019. Available in: https://ssrn.com/abstract=3384012.

HALLIDAY, Josh. Google faces new Street View data controversy. *The Guardian*, p. 379, 2012.

HICKOK, Elonnai; KHARBANDA, Vipul. *An Analysis of the CLOUD Act and Implications for India*. 2018.

HIROSE, M. Privacy in public spaces: the reasonable expectation of privacy against the dragnet use of facial recognition technology. *Conn. L. Rev*, 2016.

KOFF, E. *NSW Accellion Data Breach*. 2020.

KUNER, C. International Organizations and the EU general data protection regulation: exploring the interaction between EU Law and International Law. *International Organizations Law Review*, v. *16*, n. 1, p. 158-191, 2019. Available in: https://doi.org/10.1163/15723747-2019008.

MISHRA, Neha. Data localization laws in a digital world: data protection or data protectionism?. *The Public Sphere,* 2015.

MOSSINGHOFF, G. J.; OMAN, R. The World Intellectual Property Organization: a United Nations success story. *World Affs*, 1997.

MURTHY, M. S. Data protection law and policy in the USA: an overview. *Indian JL & Legal Research,* n. 3, 2022.

PAGOROPOULOS, A.; PIGOSSO, D. C.; MCALOONE, T. C. The emergent role of digital technologies in the Circular Economy: a review. *Procedia CIRP*, 2017.

REZENDE, I. N. Facial recognition in police hands: assessing the 'Clearview case' from a European perspective. *New Journal of European Criminal Law*, p. 375-89, 2020.

STAFF, Reuters. *Facebook loses Belgian privacy case, faces fine of up to $125 million*. Available in: https://www.reuters.com/article/us-facebook-belgium-idUSKCN1G01LG.

STREINZ, T. The evolution of European data law. *In*: CRAIG, Paul; BÚRCA, Gráinne de (ed.) *The Evolution of EU Law'OUP*. 3rd. ed. Oxford: Oxford University Press, 2021.

SULLIVAN, Clare. EU GDPR or APEC CBPR? A comparative analysis of the approach of the EU and APEC to cross border data transfers and protection of personal data in the IoT era. *Computer law & security review,* v. 35, n. 4, p. 380-397, 2019.

SVANTESSON, D. Enforcing privacy across different jurisdictions. Enforcing privacy: regulatory, legal and technological approaches. *Springer,* p. 195-222, 2016. Available in: https://link.springer.com/chapter/10.1007/978-3-319-25047-2_9.

TRACOL, Xavier. Schrems II: the return of the Privacy Shield. *Computer Law & Security Review*, v. 39, 2020.

TYAGI, A. K.; REKHA, G.; SREENATH, N. Is your privacy safe with Aadhaar?: an open discussion'. *IEEE,* Solan, p. 318-323, 2018.

UN GLOBAL PULSE. *UN global pulse principles on data protection and privacy*. Available in: https://www.unglobalpulse.org/policy/ungp-principles-on-data-privacy-and-protection/.

UNITED NATIONS. System Chief Executives Board for Coordination. *International data governance*: pathways to progress. Available in: https://unsceb.org/international-data-governance-pathways-progress. Access on: May 2023.

UNITED NATIONS. *Data strategy of the Secretary-General for action by everyone, everywhere with insight, impact, and integrity 2020-22*. 2020. Available in: https://www.un.org/en/content/datastrategy/images/pdf/UN_SG_Data-Strategy.pdf.

VOSS, W. Gregory. Cross-border data flows, the GDPR, and data governance. *Wash. Int'l LJ*, v. 29, p. 485, 2019.

WHITLER, K. A.; FARRIS, P. W. The impact of cyber-attacks on brand image: why proactive marketing expertise is needed for managing data breaches. *Journal of Advertising Research*, v. 57, n. 1, p. 3-9, 2017.

WIPO Convention. 1967. Available in: https://www.wipo.int/portal/en/index.html.

YAKOVLEVA, Svetlana; IRION, Kristina. Pitching trade against privacy: reconciling EU governance of personal data flows with external trade. *International Data Privacy Law*, v. 10, n. 3, 2020.

YILMA, Kinfe. *Privacy and the role of international law in the digital age*. 2023.

ZHAO, J; MORTIER, R; CROWCROFT, J; WANG, L. *Privacy-preserving machine learning based data analytics on edge*. 2018.

ZHENG, G. Trilemma and tripartition: the regulatory paradigms of cross-border personal data transfer in the EU, the US and China. *Computer Law & Security Review*, 2021.

ZHU, Y.; ZHONG, N.; XIONG, Y. Data explosion, data nature and dataology. *Springer Link*, p. 147-158, 2009.