NAVIGATING CROSS-BORDER DATA TRANSFERS: A COMPARATIVE ANALYSIS OF DATA PROTECTION LEGISLATION FOR BUSINESSES IN IRELAND AND KENYA.

Research dissertation presented in partial fulfilment of the requirements

for the degree of
MSc International Business and Law
Griffith College Dublin

Dissertation Supervisor: Sana Khan

Student Name: Calvin Kinyanjui

Candidate Declaration

Candidate Name: Calvin Kinyanjui

I certify that the dissertation entitled: "NAVIGATING CROSS-BORDER DATA TRANSFERS: A COMPARATIVE ANALYSIS OF DATA PROTECTION LEGISLATION FOR BUSINESSES IN IRELAND AND KENYA"

submitted for the degree of **MSc International Business and Law** is the result of my work and where reference is made to the work of others, due acknowledgement is given.

Candidate signature: Calvin Kinyanjui

Date: 28th August 2020

Supervisor Name: Sana Khan

Supervisor signature:

Date:

Acknowledgements

I thank the Lord, for His guidance which gave me resilience to carry through this dissertation and master's program. I also thank my family for being a source of unyielding support and consistent reassurance.

My gratitude is also extended to Ms. Sana Khan for her sincere guidance throughout this research.

I am also thankful for the GBS team who have provided all necessary systems of support during my master's program, and I am indebted to all those who have contributed to the development of this body of work.

Dedication

I dedicate this body of work to my family who provided support throughout my master's program.

Table of Contents

List of Figures

List of Abbreviations

AU: African Union

BRCs: Binding Corporate Rules

CJEU: Court of Justice of The European Union

DG MARKET: Directorate General of the Commission for the Internal Market

DPA: Data protection Act

DPC: Data Protection Commission

DPF: Data Privacy Framework

EAC: East African Community

ECOWAS: Economic Community of West African States

EEA: European Economic Area

ECFR: European Council on Foreign Relations

EU: European Union

GATT: General Agreement on Tariffs and Trade

GDPR: General Data Protection Regulation

GSD: Global Software Development

IOT: Internet of Things

LGPD: Lei Geral de Proteção de Dados

MNCs: Multinational Corporations

NSA: National Security Agencies

OECD: Organization for Economic Co-operation and Development

ODPC: Office of the Data Protection Commissioner

POPIA: Privacy of Personal Information Act

SCCs: Standard Contractual Clauses

TFEU: Treaty on the Functioning of the European Union

Abstract

We live in an era marked by swift digitization of businesses activities and global data transfers, safeguarding personal information across boundaries (national and supra-national) has subsequently become a crucial issue for corporations and governments alike. In "Navigating Cross-Border Data Transfers; A Comparative Analysis of Data Protection Legislation for Businesses in Ireland and Kenya," the paper seeks to critically compare and assess the legal frameworks that govern data protection legislation in the two vastly different jurisdictions. Notably, Ireland abides by the General Data Protection Regulation (GDPR), which has acted as a predecessor of data protection rules internationally and is a member of the European Union (EU). In contrast, Kenya often called the 'Silicon Savannah' functions under the framework of the Data Protection Act, 2019, a recent law that has played a significant role in the development of data protection in East Africa.

1. Introduction

1.1 Overview

There has been a considerable evolution in the world of data privacy in the last few decades, which has worked to enhance protection of personal data against unlawful access, use and disclosure. This resulted from the development of the growth of the Internet of Things (IOT) which facilitated the aggregating, processing, and distribution of data on a large scale, subsequently, ideas to regulate this activity gained traction in the late 20th century. Modern privacy standards are rooted in semblance of early data protection regulations such as the 1981 Council of Europe Convention for the protection of Individuals regarding automatic processing of personal data (Council of Europe, 1981). This paved the way for government and Multinational Corporations (MNC's) developing systems to mitigate threats of identity theft, data breaches and unauthorized surveillance. That be as it may, the development of artificial intelligence, big data and cloud computing has heightened the need for even more stringent data protection legislation and requirements. As a result, many nations have passed extensive data protection legislation to fortify security measures and ensure that MNC's utilize personal data responsibly (Gellman, 2014).

The movement of personal data over national borders is recognized as cross-border data transfers, and is frequently facilitated through cloud computing, digital communication and international business activities. While these transfers are critical for global trade, they also pose a major privacy threat, especially when data is transferred from nations with extremely rigorous data protection policies and laws to ones with lesser controls. To address these worries, the General Data Protection Regulation (GDPR), came into force in 2018 and established strict guidelines for the transferring of personal data outside the European Union. Consequently, only nations that can provide an 'adequate' level of data protection such as Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs) are permitted to engage in such transfers. These protocols guarantee that personal data is safeguarded in compliance with EU legislation, regardless of the processing or storage location. The GDPR aims to uphold strict guidelines for data privacy and security across national borders while honoring people's rights in the digital age (Kuner et al., 2020).

In Ireland, the primary law implementing GDPR regulations is the Data Protection Act 2018, It guarantees that personal data is handled in accordance with EU standards. Additionally, the supervisory regulatory body in charge of enforcing these mandates is the Data Protection Commission (DPC), it conducts audits and issues penalties for non-compliance. This regulatory framework ensures that foreign operating entities in the state preserve trust in digital transactions.

In comparison, Kenya's primary data protection legislation, is the Data Protection Act 2019, which came into effect in November of the same year. It effectively introduced the state into a new data privacy dispensation that aimed at upholding the integrity of all Kenyan persons, and governing MNCs operating within the jurisdiction. Largely modeled against the GDPR, it became one of the few countries in Africa to join the global standard for data protection.

1.2 Research Purpose

The primary objective of this study is to conduct a thorough comparative analysis of Irish and Kenyan data protection legislation, with an emphasis on cross-border data transfers and security. The research focuses on the current digital landscape, where data flows are re-defining modern existence, and data privacy laws serve as indispensable benchmarks, delineating the rules that govern the collection, processing, and sharing of personal information (Chander & Schwartz, 2023). As such, it will examine the impact on enterprises and assess policies to improve and leverage security and compliance.

Additionally, the study will also analyze the concepts around allowing data flows by default; establishing base-level layers of protection for all global players; prioritizing cyber security; incorporating diplomacy in the hardwiring of accountability among nations and prioritizing connectivity and technical interoperability alongside data provenance and portability. This is extremely important, as all these facets are inextricable from the fourth industrial revolution which is 'the current period of rapid, simultaneous and systemic transformations driven by advances in science and technology – reshaping industries, blurring geographical boundaries, challenging existing regulatory frameworks, and even redefining what it means to be human.' (World Economic Forum, 2017).

Finally, regulatory authority bodies alongside policy analysts and scholars acknowledge the developing clash between the commodification of personal data and the existing body of regulations that govern the data (G20, 2019). This demonstrates that there is need to combine these two impulses considering the growth of the digital economy, and that both call for intergovernmental involvement. The challenge therein lies in adopting regulatory standards that simultaneously secure privacy and data protection (Svantesson, 2020), while removing potential barriers to cross-border information transfers when it is necessary to facilitate them. This study will contribute to the discussion around cross-border data protection by providing insights that can assist align national frameworks, lived experiences and growing global best practice.

1.3 Significance of the Study

This study is important as it will assess the quickly developing need for effective and consistent regulated data protection mechanisms in the current 'digital age,' where cross-border data transfers are interwoven in day-to-day business operations. It analyzes the need for a global data convention, that would effectively develop a cohesive collection of data standards and principles that bring together national governments, public institutions, the commercial sector, academic institutions, and civil society organizations to have a harmonized playing field.

This study will also provide legislators with vital information and assist them in reviewing the intricate balance between data mobility and the data protection laws. By exploring the specific circumstances of Ireland and Kenya, this study will not only contribute to the existing body of knowledge but will also establish practical and implementable solutions for other jurisdictions facing similar issues.

1.4 Research Objectives

This study was arrived at by questing the current landscape of data protection from both a business and legal perspective. The driving question was, "How do the data protection legislation frameworks in Ireland and Kenya differ in regulating cross-border data transfers, and what are the

implications of these differences on Multinational Corporations (MNCs) operating in these jurisdictions?" This provided the following research objectives:

1. To conduct a comprehensive comparative analysis of the data protection legislation on Ireland and Kenya, with a particular focus on the regulatory frameworks governing cross-border data transfers.
2. To assess the implications of these data protection laws while identifying the specific challenges and opportunities for MNCs and regulatory bodies operating in both jurisdictions.
3. To develop recommendations for enhancing data protection practices in Ireland and Kenya, with the aim of improving best practice, cross-border security and harmonized operational efficiency.

1.5 Structure of the Study

This study is broken down into five central chapters covering different concerns highlighted as follows: Chapter one introduces the research topic and lightly discusses the significance of data protection and the regulation of cross-border transfers in today's global economy; chapter two intensively analyzes the existing literature and relevant legal frameworks that have actively mapped and governed data protection and cross-border data transfers; chapter three outlines the research methods and designs applied to the study, the comparative legal research methodology, the selection criteria for academic texts and the data gathering procedures; chapter four represents the findings and results from the comparative analysis, interviews, and the general study and chapter five will conclude on the important findings of the research, reflecting the study's contribution to the field of data protection and cross-border data governance.

2.0 LITERATURE REVIEW

2.1 Overview

The commodification of personal data has enabled digital trade and actively contributes to economic development, whilst meeting the needs of the protracted parties (data subjects, data processors and data controllers). That be as it may, those benefits are jarringly removed from the realities of the threats posed to data subjects when their personal data is abused through identity theft, surreptitious monitoring, racial profiling, denial of necessary services, and persistent marketing through cookie use. Notably, a more concerning element of this reality is the transferability and re-utilization of this data, which can not only be sold but also presented in various forms at the same time in many locations while users are still unaware of this violation of privacy. According to Seeman and Susser (2024) a wide range of individuals are involved in privacy regulation, from lawmakers and government agencies to privacy engineers. Although regulators often draft privacy laws, technical players within businesses are crucial to implementing said laws "on the ground" and sometimes even through privacy-enhancing technologies. This translates to the data collected being subjected to the ‘ethics and ‘moral fabric’ of data handlers who oversee compliance regulations. These individuals are tasked with what equates to essential processing and utilization of the data while balancing the internal goals of their employer’s firms and the external pressures of the law.

Companies engaging in international markets face the challenge of compliance with multitudes of data protection regimes and regulations for cross-border transfers (Ethics & Compliance Initiative, 2021). These entities benefit from arguments of actively dismantling and reconciling restrictions for the free flow of data whilst pushing the narrative that such stringent policies are an active barrier to economic growth for ‘first world countries’ to ‘developing countries’ and ‘third world countries.’ This is a result of the shift in the economic theory of regulation, most paired with the school of neoliberal thought on digital protectionism, (Ruggie, 2017). Trade economists and international lawyers affiliated with the GATT (Gamble, 2013), suggests that any regulation may constitute a barrier to trade, which negates the public interest

theory which argues that regulations may be adopted in the public interest, primarily to correct market failures and achieve societal goals (Ginosar, 2014). This therefore strongly suggest that the

former is of more importance and relevance to any developing economy as it ensures a 'holistic' market capture, accommodating the needs of all citizens rather than pricing out individuals that may potentially benefit from such trade. Nevertheless, legal practitioners and regulatory authorities understand the integral need to establish checks and balances to avoid catastrophic repercussions in the future.

2.2 Data Security and Privacy Framework.

Over the years, the vulnerability of data security and computer systems has steadily developed, given the rise of malicious cyber-attacks and hacking dangers by rogue organizations and individuals (Khan et al., 2022). The digital ecosystem's interconnectedness demonstrates that traditional methods of protecting privacy are rapidly proving insufficient towards advancing technical risks. This is further observed through the overlapping of technological development and the world of privacy law (Chugh, 2023); as such, legal frameworks are fast becoming redundant in curbing malpractice and the prolonged periods required to implement new laws, cannot match the unregulated environment that newer and more aggressive inventions such as artificial intelligence are unethically navigating and taking over. Lyon (2014), provides that the Snowden revelations about National Security Agency (NSA) surveillance, starting in June 2013, alongside the ambiguous complicity of internet companies and the international controversies that followed, illustrate the ways that Big Data has a supportive relationship with covert surveillance and noncompliance. This argument highlights the constant interference by "rogue governments and companies" incentivized by a hunger for power in the new age of data revolution overrides legal provisions and the moral code of conduct expected in the international arena.

According to Obaidat et al., (2020) in his research paper on security frameworks on the IoT, through confidentiality, integrity, and availability (C-I-A Triad) security concerns may be curbed, as this only allows authorized and trained data processors to have access to certain data, who then encrypt and modify data for transmission, processing and storage and finally erasure in a timely manner. This is merely a step towards the data integrity that is expected at a global scale, unfortunately, it not the lived experience as these baseline frameworks are unattainable to not only businesses, but also certain governments that are forced to use technology systems that are

outdated and face budgetary constraints to bring on the necessary talent and man power to enforce this regulations.

2.2.1 Develpoment of EU-Irish Data Privacy Framework.

The right to protection of personal data became a legally binding fundamental right for all member states of the European Union in 2009, when the EU Charter came into full effect. (European Union, 2012). Notably, this was after its predecessor the 1995 Data protection Directive (European Parliament and Council, 1995), whose dual goals were to safeguard the individual's fundamental freedoms and rights, including the right to their personal data, and to guarantee the unhindered free flow of data within the European Economic Area (EEA). At the time, the notion of a threatened digital sovereignty resulting from digital trade was almost non-existent as the IOT was relatively new and MNC's had adequate regulations. However, concerns soon developed after the growing power of offshore companies having access to unregulated data, especially those that operated with ideological differences (Bongiovi, 2019). This in turn exacerbated the introduction of the GDPR, which ensured adequacy control as a mitigative measure to developing threats.

The data privacy framework in Ireland was more rigorously challenged because of the Shrems I and II cases. The argument in Shrems I (Case C-362/14, *Maximillian Schrems v Data Protection Commissioner*, 2014) was that the EU/US legal instrument (Safe Harbour Agreement) was invalid, this was founded in a controversy relating to Facebook. The CJEU was tasked with assessing whether a Data Protection Authority (DPA) was prevented from investigating individual complaints related to an EC decision and legal instruments based on it, even in the wake of violations to the provisions of Article 25(6) of Directive 95/46 and Articles 7, 8 and 47 of the European Charter of Fundamental Rights (ECFR). The CJEU ruled that national DPAs (Data Protection Authority) have the right to investigate individual complaints related to the EC decision and legal instruments linked to the decisions, and notably declared the Safe Harbour Agreement invalid.

Similarly, in Shrems II (Case C-311/18, *Data Protection Commissioner v Facebook Ireland Ltd, Maximilian Schrems*, 2018), Maximillian revised his complaint to the Irish DPA, stating that the Standard Contractual Clauses (SCCs) decision did not support the transfer of personal data to the US, because US monitoring programs actively interfered with his fundamental rights to data

protection, privacy and efficient legal protection. The DPA filed case with the Irish High Court, which requested a preliminary hearing from the court to assess the validity of the Privacy Shield Decision (an alternative transfer mechanism), which was ruled as illegitimate the CJEU. This decision informed the digital landscape of the high-level SCCs required to facilitate cross-border data transfers. More recently, Jourová, (2023), while addressing the European Commission highlighted that, "the GDPR has become a new benchmark for effective data protection law globally and it is the enforcement of the law that will decide on its full success," solidifying the argument the fact that corporate compliance is of utmost importance.

2.2.2 Development of Africa-Kenyan Data Privacy Framework.

The African union (AU) finally unveiled its eagerly anticipated African Union Data Policy Framework (DPF) on July 28, 2022 (King'ori, 2024). The framework aims to protect African countries' interests while promoting the use of data for purposes of growth and innovation, and its core areas of focus are cyber security, data governance, e-commerce and the protection of personal data and information. To achieve continental constructive collaboration of data-related policies, the DPF strongly recommended the utilization of the already existing regional blocks of member nations. Notably, this paved way for the revision of the ECOWAS Act (ECOWAS, 2023), which intends to amend the supplementary Act to address both new and existing data protection issues, and to emphasize data harmonization and cross-border data flows to increase member state capacity (Babalola, 2024). Additionally, this is built on the foundation of the Malabo Convention (African Union, 2014), which was guided by the constitutive Act of the African Union adopted in the year 2000. This Convention served to reaffirm the commitment of member states to fundamental freedoms and human rights contained in declarations and other instruments adopted by the African Union and United Nations.

The right to privacy is enshrined in Article 31 of the Kenyan constitution (Kenya Law Reform Commission, 2010). It provides that; 'Every person has the right to privacy, which includes the right not to have their person, home or property searched; their possessions seized; information relating to their family or private affairs unnecessarily required or revealed; or the privacy of their communications infringed.' This is the blueprint upon which the Data Protection Act 2019 which came into effect in November 2019 was built (Bowmans, 2019).

2.3 Data Protection Legislation

According to Greenleaf, (2021) in the paper assessing EU legislation and its impacts on the international space, provided that, data protection legislation defines the complex and ever evolving framework of laws and regulations designed to protect the privacy and personal data of individuals across different jurisdictions. These laws act as the guiding framework of how personal data is collected, processed, stored, and transferred across different jurisdictions while upholding 'data sovereignty.' Voigt and Bussche (2021), argue that the current highest possible standard of data regulation internationally is modelled against the General Data Protection Regulations. In this light, various international players have enacted laws to meet new international standards. Two of the developing BRICS countries, Brazil and South Africa have passed their own comprehensive data privacy laws known as Lei Geral de Proteção de Dados (LGPD) (Belli et al., 2020) and the Privacy of Personal Information Act (POPIA) (Staunton et al., 2020), respectively. The recent legislation in the afore mentioned jurisdictions has inter alia provided more regulatory power and defined security for citizens especially where cross-border data transfers matters are involved with MNCs.

It remains unclear whether simply enacting laws and establishing regulatory bodies will be enough, it is however a step closer to improved data governance and enhanced corporate responsibility and transparency. Kuner (2020), highlights that the onset of stricter data protection laws fosters international collaboration in the enforcement of standards and the confidence in digital economies.

2.3.1 The General Data Protection Framework (GDPR)

The Directorate General of the Commission for the Internal Market ('DG MARKT'), (European Commission, 2003) published its first report on the implementation of the Data Protection Directive (95/46/EC), (European Commission, 2003) to facilitate a more comprehensive framework and put in place systems to govern data protection within the EU. Six years later in 2009, the treaty of Lisbon (EUR-Lex, 2009) introduced the right to data protection with a specific legal basis for data protection legislation in Article 16 of the Treaty on the Functioning of the European Union (TFEU) (FRA, 2009) which increased oversight of and participation in data

protection alongside policy-development by the European Parliament, effectively elevating the Charter of Fundamental Rights (CFR) to the EU.

Following the rapid digitization of the economic and market in the EU, the Directorate General for Justice (DG JUST), in 2011 commissioned services of an internal consultative draft of the GDPR, which was adopted in 2012 based on Article 16(2) TFEU as an ordinary legislative procedure. The GDPR came into effect in 2018 and was quickly adopted as the global standard Data Protection 'handbook.' Unsurprisingly, the GDPR marked a transition into canonical shifts elevating cyber security, data governance, privacy compliance, technological development, monitored personal data utilization and risk management (Dickhaut et al., 2023). All MNCs operating on European soil would devote a significant amount of labor and funds to modernizing their digital platforms, revising their privacy rules, altering their advertising strategies, and modifying their data processing and storage procedures (Li, Yu, and He, 2019). As a result, the market saw fresh players whose subject matter expertise was a cross-section of business, law, and technology regulation.

2.3.2 Ireland's Data Protection Act 2018

The Irish Data Protection Acts 1998 (Data Protection Act 1988) and 2003 (Data Protection (Amendment) Act 2003) were superseded by the Data Protection Act 2018 (Data Protection Act 2018) which gave effect to the limited areas of flexibility permitted under the General Data Protection Regulation (GDPR), transposing the law enforcement Directive into Irish law, whilst replacing the Data Protection Commissioner with the Data Protection Commission and providing for consequential amendments to various Acts that contain references to the Data Protection Acts 1988 and 2003 (Data Protection Act 2018 Explanatory Memorandum, 2018).

Kelleher, (2020) in their academic journal contributes that the Act is particularly significant given Ireland's role in the European Market post Brexit, owing to the vast number of technology powerhouses having operational headquarters in the country. This solidified Ireland as a global digital hub while simultaneously increasing the GDP. The DPA 2018 reinforced the principles of data protection, among them being; adequacy, consent, legitimacy, and accountability. That be as it may, there has been criticism about the operational efficiency of the DPA's monitoring authority, the DPC. Murphy (2020), in her paper concludes that although the DPC can enforce data protection laws and apply fines, the office appears to veer from taking decisive and swift action against MNCs.

To add to this, legal experts have raised alarm over the Act's excessively broad rules on data processing for national security goals, which may be used to infringe on privacy rights (O'Hara, 2019). This reflects poorly on the countries' measures to mitigate and actively address any data privacy challenges, as previously noted in Shrems I and II cases. The DPA 2018's efficacy is inextricable from the DPC's capacity to oversee its caseloads and establish its authority. That be as it may, it has proven adequate in handling investigations and performing its role as a regulatory authority body.

2.3.3 Kenya's Data Protection Act 2019

Article 31, of the Kenyan Constitution (Kenya Constitution, 2010) protects the right to privacy, it provides that every individual has the right not to have their person, home or property searched; their possessions seized; information relating to their family or private affairs unnecessarily required or revealed; or the privacy of their communications infringed. This serves as the foundation upon which the Data Protection Act 2019, draws its constitutional mandate. The Act remains a landmark piece of legislation in Kenya that set precedence in the East African and the grater African region as well. It came into effect just a year after the GDPR, which it was modeled against, with the goal to align itself with international standards and in response to the growing need of privacy concerns and data protection in both the private and public sectors (Gichuhi, 2020).

Alongside the legislation, the Office of the Data Protection Commissioner (ODPC) was created to oversee data security and enforce the law in respect to the Act's provisions (Office of the Data Protection Commissioner, 2021). Additionally, the Data Protection (General) Regulations, 2021 (Kenya Gazette Supplement No. 236, 2021), cover the rights of data subjects, the obligations of data controllers and processors to uphold these rights, and precise instructions on how to apply regulatory action, enabling wider enforcement of the Act (Mweu, 2022).

Nyaga (2021) provides that, while assessing data privacy and vicarious liability in the Kenyan landscape, questions the enforceability of the office of the Data Protection Commissioner, siting budgetary constraints and lack of structural independence, while (Mwangi 2020), critiques the exemptions of national security bodies allowing derogations for where best deemed fit. Whilst these are founded concerns, they fail to account for the fact that the office has been in operation for only three years and as such, compounded risks will be difficult to handle all at once, more so

as the digital landscape is, and privacy law is young. Additionally, the ODPC has achieved a great deal within the three years and the silicon savannah (Kenya), is still championing global standards in Africa.

2.4 Cross Border Data Transfers

Adequately captured by Kuner (2019), the EU framework governing transfer of personal data outside the EEA is based on a 'prohibition with derogation' principle. Transfers of personal data to a country or territory outside the EEA or to an international organization may only occur if the conditions in Chapter (V) of the GDPR are met. Yakovleva (2022), adds that, although the concept of 'transfer' is central in triggering the application of restrictions on the transfer of personal data, neither the GDPR nor its predecessor-the Data Protection Directive- defines the concept of 'transfer' of personal data outside the EU. As such, there is a broad interpretation of what transfer of personal data for "necessary action" may be for MNCs, allowing for data misuse and lack of corporate accountability. This grey zone was, however, subject to correction as was seen in the Shrems II case where the CJEU and the European Data Protection Board (EDPB) (European Data Protection Board, 2018) provided that:

i) 'Granting direct access to a database (e.g. via and interface an IT-application) on a general basis constitutes a transfer of personal data in the meaning of the GDPR (European Data Protection Board, 2018), and
ii) Data in transit is equally subject to the rules on transfer of personal data outside the EEA under the GDPR (Court of Justice of the European Union, 2018).

Between 2021 and 2023 the EDPB published guidelines with the goal to effectively capture rules for transfers, and the results garnered critique, nevertheless, the data protection authorities and courts across the EU accepted them whilst noting they were not legally binding (European Data Protection Board, 2021).

The GDPR has so far acted as the guiding framework for the governing of data flows, and while various scholars may argue against its efficiency, it has reflected that its enforcement has changed how international organizations, regulatory authority agencies and the international market views

privacy requirements. Tosoni (2020), highlights that the GDPR 'cross-border processing' means either:

i) Processing of personal data which takes place in the context of activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member state; or
ii) Processing of personal data which takes place in the context of activities of a single establishment of a controller or processor in the Union, but which substantially affects or is likely to substantially affect data subjects in more than one Member state.

The interpretation of these provisions is that despite data processing being clear, complexity may arise from the 'substantiality' of the impacts of processing on data subjects from different jurisdictions in the EEA.

2.4.1 Cross-Border Data Transfers in Ireland

The General Data Protection Regulation (GDPR) and other pertinent EU directives are implemented and supplemented by the Data Protection Act 2018, which serves as the main legislative framework for data protection in Ireland. Murphy (2018) in her article, notes that it is important to remember that in every member state, including Ireland, national legislation is superseded by the GDPR as an EU rule, and in support of her argument, this indicates that the GDPR continues to be the primary legislative framework for data protection throughout the EU, even while the Data Protection Act of 2018 has certain provisions and modifications tailored to the Irish environment.

In this light, the GDPR provides that, "any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organization shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in Chapter V are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organization to another third country or to another international organization. All provisions in Chapter V shall be applied to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined." (GDPR, 2018).

The wording of this specific provision stresses the inextricable dynamic between the law and inter alia data processors and data controllers operating in different jurisdictions, despite the existence of extraterritorial provisions that may lack harmonization with the GDPR. While this raises equity questions on the global landscape, in constructive collaboration with the "Brussels Effect," the European Union, according to Bradford (2012), is creating international regulations in several sectors, including antitrust, privacy, health protection and environmental protection. The author emphasizes that the EU has set the tone in privacy protection, and consequently MNCs amongst other international players realize that data flows are contingent on meeting adequacy requirements.

In line with best practice the GDPR's Articles 45-50, provide the relevant requirements for cross-border data transfers, this study will assess Article 45 as it is the most enforced in comparison to the remaining provisions. Article 45 (GDPR, 2018) Provides:

1) "A transfer of personal data to a third country or an international organization may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organization in question ensures an adequate level of protection. Such a transfer shall not require any specific authorization.
2) When assessing the adequacy of the level of protection, the Commission shall take account of the following elements:

    a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organization which are complied with in that country or international organization, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;
    b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organization is subject,

with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and

c) the international commitments the third country or international organization concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.

3) The Commission, after assessing the adequacy of the level of protection, may decide, by means of implementing act, that a third country, a territory or one or more specified sectors within a third country, or an international organization ensures an adequate level of protection within the meaning of paragraph 2 of this Article. The implementing act shall provide for a periodic review mechanism, at least every four years, which shall consider all relevant developments in the third country or international organization. The implementing act shall specify its territorial and sectoral application and, where applicable, identify the supervisory authority or authorities referred to in point (b) of paragraph 2 of this Article. The implementing act shall be adopted in accordance with the examination procedure referred to in Article 93(2).

4) The Commission shall, on an ongoing basis, monitor developments in third countries and international organizations that could affect the functioning of decisions adopted pursuant to paragraph 3 of this Article and decisions adopted on the basis of Article 25(6) of Directive 95/46/EC.

5) The Commission shall, where available information reveals, in particular following the review referred to in paragraph 3 of this Article, that a third country, a territory or one or more specified sectors within a third country, or an international organization no longer ensures an adequate level of protection within the meaning of paragraph 2 of this Article, to the extent necessary, repeal, amend or suspend the decision referred to in paragraph 3 of this Article by means of implementing acts without retro-active effect. Those implementing

acts shall be adopted in accordance with the examination procedure referred to in Article 93(2). On duly justified imperative grounds of urgency, the Commission shall adopt immediately applicable implementing acts in accordance with the procedure referred to in Article 93(3).

6) The Commission shall consult with the third country or international organization to fix the situation, giving rise to the decision made pursuant to paragraph 5.

7) A decision pursuant to paragraph 5 of this Article is without prejudice to transfers of personal data to the third country, a territory or one or more specified sectors within that third country, or the international organization in question pursuant to Articles 46 to 49.

8) The Commission shall publish in the *Official Journal of the European Union* and on its website a list of the third countries, territories, and specified sectors within a third country and international organizations for which it has decided that an adequate level of protection is or is no longer ensured.

9) Decisions adopted by the Commission based on Article 25(6) of Directive 95/46/EC shall remain in force until amended, replaced, or repealed by a Commission Decision adopted in accordance with paragraph 3 or 5 of this Article."

Kuner (2020) poses that the adequacy decision mechanism is extremely critical as it simplifies processes, while exempting data exporters from the requirement of additional safeguards. Interestingly, despite the clear representation of adequacy requirements, the Unites States, one of the "most" technologically advanced and regulatory compliant players in the international space, had the privacy shield (International Trade Association, 2017), struck down and pronounced invalid by the CJEU, only a year and a half after the privacy shield succeeded the Safe Harbour Framework (Federal Trade Commission, 2015), which was subjected to the same fate. This resulted from the Irish DPC pursuing investigations and later litigating against Facebook Ireland on the grounds of meeting EU standards on privacy requirements (Schrems II, 2020).

2.4.2 Cross-Border Data Transfers in Kenya

The primary legislation governing cross-border data transfers in Kenya is the Data Protection Act 2019 (Data Protection Act, 2019), which was enacted in alignment with the GDPR for the harmonization of Kenya's data protection standards and international best practice. The laws enacted in the Act, work in compliment with the Consumer Protection Act (Consumer Protection Act, 2012), pursuant of article 46 of the constitution of Kenya. The organization for Economic Co-operation and Development (OECD) guidelines for multinational firms, which are government recommendations for multinational enterprises on responsible corporate conduct, served as a model for this legislation (OECD, 1999). The legislation imposes the duty on data controllers and processors to ensure data is processed fairly, lawfully, transparently and with the express consent of data subjects.

Chapter VI of the Data Protection Act (Data protection Act 2022), is responsible for the regulation of transfers outside Kenyan Jurisdiction, it provides:

48. “Conditions for transfer out of Kenya;

1) the data controller or data processor has given proof to the Data Commissioner on the appropriate safeguards with respect to the security and protection of the personal data;

2) the data controller or data processor has given proof to the Data Commissioner of the appropriate safeguards with respect to the security and protection of personal data, and the appropriate safeguards including jurisdictions with commensurate data protection laws;

3) the transfer is necessary;
    a) for the performance of a contract between the data subject and the data controller or data processor or implementation of precontractual measures taken at the data subject's request;
    b) for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another person;
    c) for any matter of public interest;
    d) for the establishment, exercise or defense of a legal claim;

e) in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; or
f) for the purpose of compelling legitimate interests pursued by the data controller or data processor which are not overridden by the interests, rights, and freedoms of the data subjects

49. Safeguards prior to transfer of data out of Kenya;

1) The processing of sensitive personal data out of Kenya shall only be affected upon obtaining consent of a data subject and on obtaining confirmation of appropriate safeguards.
2) The Data Commissioner may request a person who transfers data to another country to demonstrate the effectiveness of the security safeguards or the existence of compelling legitimate interests.
3) The Data Commissioner may, to protect the rights and fundamental freedoms of data subjects, prohibit, suspend, or subject the transfer to such conditions as may be determined.

50. Processing through a data server or data center in Kenya;

The Cabinet Secretary may prescribe, based on grounds of strategic interests of the state or protection of revenue, certain nature of processing that shall only be affected through a server or a data center located in Kenya."

According to Gitari (2020), in his paper assessing consumer protection in Kenya's digital economy, the lack of recourses in the office of the Data Protection Commissioner makes it extremely difficult to monitor compliance and enforce the Act's requirements. He adds, the restriction poses queries on how the law will be applied and to what extent personal data will be protected. In support of his views, Ziwa (2022), in her research on the effectiveness of legal frameworks protecting personal data in Kenya, poses questions on her discovery around the ambiguity of regulations for cross-border data transfers, especially on what constitutes as "adequate frameworks." Notably, both academics present valid arguments, especially when the state has been subjected to unignorable data-related scandals during elections (Privacy International, 2018), the roll-out of unconstitutional "second identity cards" King'ori (2021), and the purchase of citizens biometric data (Muturi, 2023).

Notwithstanding these critiques, Kenya gains from the DPA 2019, the Act boosts consumer confidence in digital transactions and offers a clear legal framework (albeit subject to significant revisions) for data protection which is essential for interoperability in e-commerce. The Office of the Data Protection Commissioner has engaged in countless training activities across the country and has effectively penalized offenders of the Act, imposing hefty fines worth millions of shillings.

2.5 Conceptual Framework

The Intellectual instrument used by a researcher to examine a study is known as a conceptual framework, showing the researcher's understanding and suggested methodology regarding a specific subject being examined. Adom et al., (2018) describes it as a blueprint of the complete research process, through which important aspects of the study are aptly presented in pictorial form, allowing for a case to be made on the significance of the study while depicting the study design. The conceptual framework of this study was developed through the assessing of the question: How do the data protection legislation frameworks in Ireland and Kenya differ in regulating cross-border data transfers, and what are the implications of these data transfers on the operation of MNCs in these jurisdictions?

Using the study, the independent variable was cross-border data legislation, whilst the dependent variable was implications on MNCs operations. The moderating variables were supervisory regulatory bodies, enforceability of the law, penalties (fines) imposed and unregulated technology practices and products. The mediating variables were the harmonization of international law and corporate responsibility (best practice).

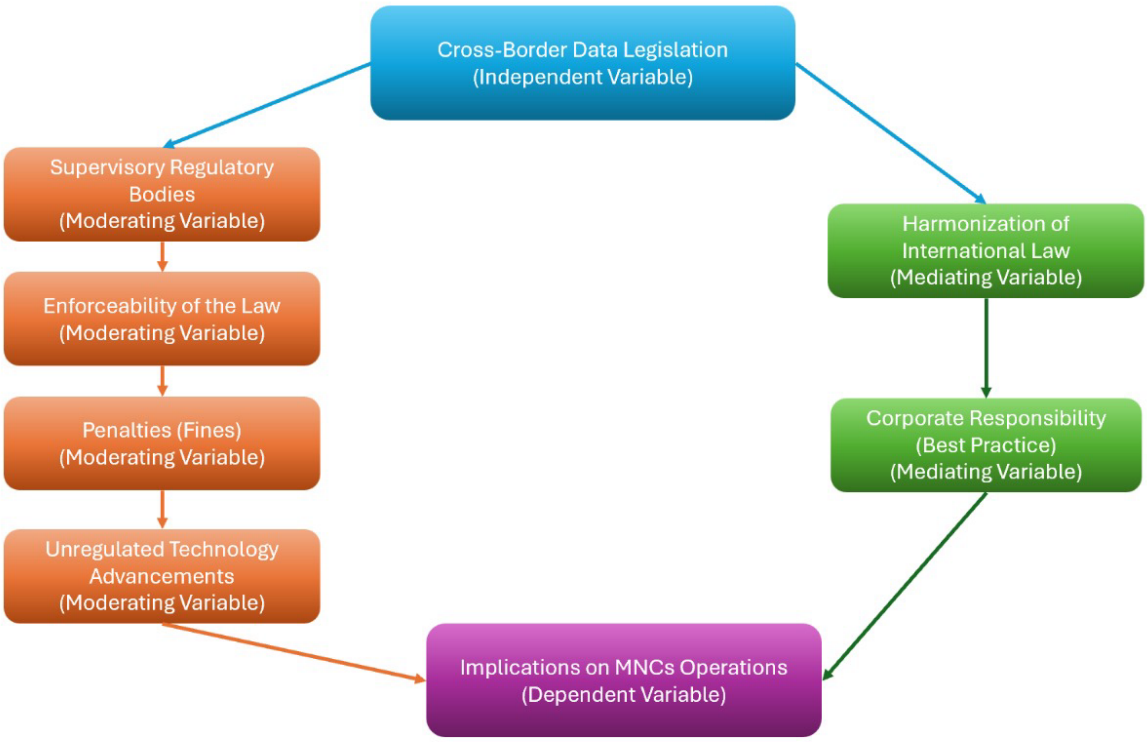

Fig 1. Conceptual framework.

2.6 Conclusion

This chapter of the study analyzed the existing sources of data privacy law and scholarly opinions, alongside the overlapping elements that influence cross-border data transfers. It highlights the critical significance of personal and other data in the global digital economy, whilst contrasting it with the clash of existing privacy laws; corporate pressure for free data flows; disharmonized international requirements; varying adequacy regimes and regional differences on data sovereignty. Notably, the findings of this chapter hold that the GDPR is currently the most important and internationally adopted framework for governance as suggested by the “Brussels Effect.

3.0 Research Methodology and Design

3.1 Overview

This chapter of the study covers the approach, philosophy and methodology applied in this study in great length. The research methodology and design are vital components of the rubric that contribute to the efficacy of a study by ensuring verifiability and reliability of a research study. A well-developed methodology provides a blueprint for data collection, analysis, interpretation and conclusion. Additionally, a coherent methodology serves as a tool of transparency, allowing supervisors and readers alike to understand the work from its onset to its conclusion and presentation.

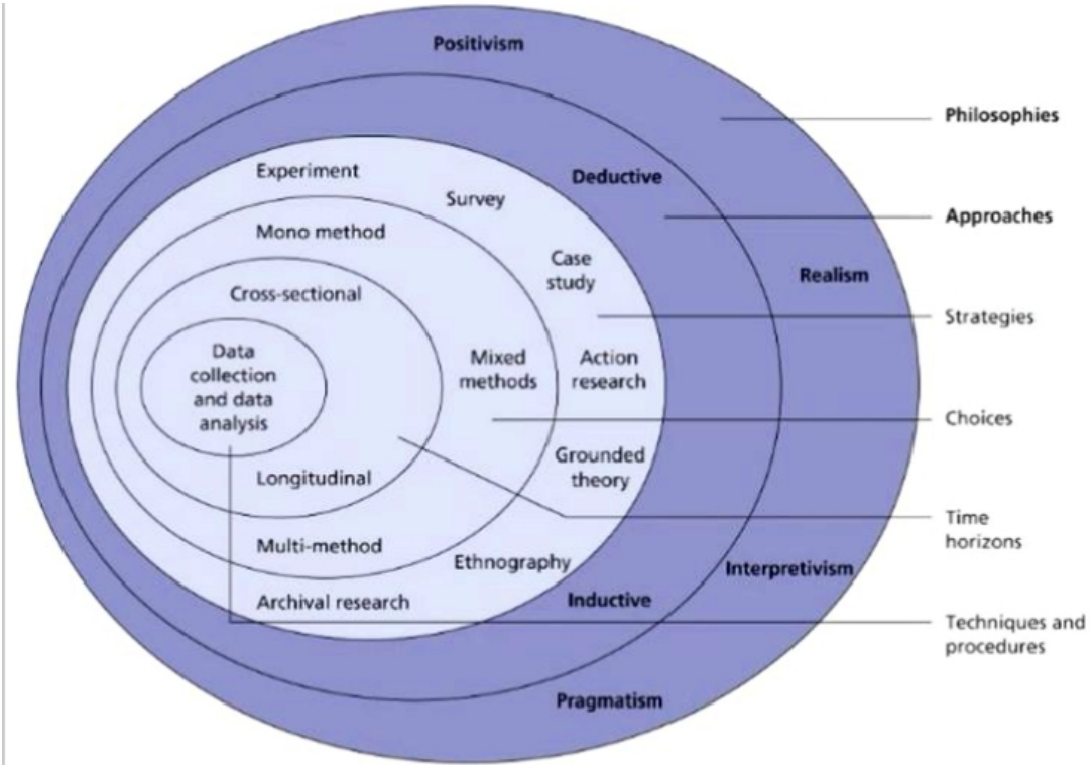

Fig 2. Research Onion (Saunders, Lewis & Thornhill, 2015, p. 124)

3.2 Research Philosophy and Approach

In his book, Saunders et al., (2015), elucidates that the research philosophy a researcher adopts, contains important assumptions about how they view the world, and these assumptions naturally underpin the research strategy and methods they will select as part of their strategy. He goes on to add that, in part, the philosophy adopted will be influenced by practical considerations, they are not, however, exempt of cognitive biases. Notably, four fundamental philosophical methods apply to epistemological and ontological assumptions: interpretivism, pragmatism, positivism, and realism. (Saunders et al., 2019).

The philosophy adopted for this study is interpretivism. Interpretivist ontology takes a relativist approach, emphasizing intersubjectivity and meaning in the study comprehension of social and experiential elements. As such, reality can only be described in a socially developed sense. Saunders et al., (2012 present that, Interpretivism, like critical realism, developed as a critique of positivism from a subjectivist perspective. Interpretivism emphasizes that humans are different from physical phenomena because they create meanings. Interpretivists study these meanings. Interpretivism emerged in early- and mid-twentieth-century Europe in the work of German, French and occasionally English thinkers and is formed of several strands, most notably hermeneutics, phenomenology, and symbolic interactionism. Interpretive research aims to enrich our understanding of social worlds and situations. It is best suited for this study, which involves the comparative analysis of two jurisdiction's laws.

The realism research philosophy relies on a long-standing school of thought that emphasizes independence of reality from the human mind. Saunders et al., (2015), presents that it is broken into two distinct groups; Direct realism can be described as "what you see is what you get." It is used to portray the world through human senses that are corruptible. Critical realism, on the other hand, argues that humans do experience the sensations and images of the real world. According to critical realism, sensations and images of the real world can be deceptive and they usually do not portray the real world. This philosophy is best suited for quantitative research and therefore cannot be adequately employed to guide this research.

In complement to the interpretivist philosophy, this study will adopt the desk-based comparative legal research method while applying the contextual integrity framework and the realist law theory.

The contextual integrity framework developed by Nissenbaum emphasizes the need to maintain and respect privacy while focusing on the dire need for categorical awareness. In the past few decades, there has been a radical intensification in the social practices of gathering, storing, manipulating, and sharing information about people's personal information. In many instances, new practices have aroused suspicion, indignation and protest among legal experts, social critics, privacy advocates and popular media in the public (Nissenbaum, 2009). This framework blends well with this study, emphasizing the growing consciousness among the masses about the need to ensure data privacy in a globalized world. The framework has been applied by regulatory agencies while notifying businesses alongside the general masses of the need to establish secure channels to disallow the misuse of personal data.

Additionally, the legal positivism theory, developed by H.L.A Hart, strongly suggests that the laws governing man are created by man himself, and as such, they are not centered around objective morality, for man is flawed. It further spells that the law's main objective is establishing and maintaining order and social stability (Legal Theory, 2000). To fully understand the theory, one must evaluate the paradigms that have broken down through three separate perspectives these are;

1) Understanding legislation from the standpoint of those who must abide by the rules which Hart refers to, as an internal point of view perspective, this is important because it highlights how people learn to embrace and interpret the laws.
2) The difference between primary and secondary roles is also attributed to Hart, noting that the former imposed rights and obligations and while the latter lays out processes for creating, modifying and resolving conflicts with fundamental norms.
3) The separability thesis as explained by Hart, clarifies the relationship between morality and the law. He suggests that the law and morality overlap remain separable institutions independent from one another. Legal validity does not depend on moral correctness. (Yeon, 2019).

This theory. Will be used to effectively assess how the laws provided in the Data Protection Acts and other legislation of both states affect businesses. More so through the lens of those governing said businesses alongside those affected by it.

3.3 Research Strategy

Saunders et al., (2019) provides that in academic research, selecting an appropriate research strategy is pivotal for the success of any study. A well-chosen research strategy guarantees that the research questions are properly addressed and that the research design is consistent with the study objectives. Importantly, theory information is strongly related to study design, and it can be deductive or inductive. And deductive approach begins with a theory or hypothesis which is tested empirically, while an inductive approach creates a theory based on observed patterns. The distinction is made between qualitative and quantitative research methodologies. The approach to be applied for this study is qualitative and inductive methodology. An inductive approach is outlined. The inductive technique begins with observations rather than preconceived theories and hypothesis, and it is supported by three major steps.

This study will use the deductive approach to examine the hypothesis derived from the theories while enabling said theories to meld with the data itself. This method is highly beneficial for exploring and cross-examining information with current ideologies. The benefits of taking this approach are its generative nature, which enables theoretical development and observational insights. It allows the researcher and interviewees to explore specific contexts and occurrences while also allowing for consistent data revisions.

3.4 Collection of Primary Data

This study will involve the collection of both primary and secondary data. Constitutions, legislation, case law, and interviews will be used as primary data sources, with legal reviews and published scholarly work serving as secondary sources. That be a sit may, for the purposes of this research chapter, the source that will be discussed is the interview, as it will involve “external” engagement.

3.4.1 Sources of primary data: Interviews

Interviews are a qualitative research technique that involves conducting thorough individual dialogue with a few numbers of respondents to investigate their perspectives on a certain topic, program, or issue. In this light, this study will apply two interview techniques:

1) Structured Interviews: Comprising a predetermined set of questions to maintain uniformity across the interviews. Especially considering that the participants being interviewed are from different jurisdictions, this will be incredibly valuable for comparing data on the larger sample.
2) Semi structured interviews: A set of questions allowing for flexibility in directing the discourse while allowing interviewees to elaborate issues of interest. They are applied in the second half set of the interview questions.

The rationale behind using interviews was to gain depth and insight. Allowing the parties to delve into the nuances of business, legal and technological practices affecting cross-border data transfers in both jurisdictions. The questions were developed by analyzing best practices in both jurisdictions. In Ireland, this involved interviewing barristers and solicitors with a data privacy background, while in Kenya, this involved interviewing advocates familiar with the Data Protection Act 2019 and the relevant case laws developed after 2022. This approach would allow for expert opinion and practical experience to be captured in both sets while allowing for themes to be developed for purposes of cross-referencing between the two jurisdictions.

It also provided flexibility, allowing the researcher to probe further into areas of interest that developed over the conversation. This was crucial in exploring new themes and arguments presented by the interviewees. Finally, it allowed for the capturing of opinions by experts who have authoritative perspectives in their fields, through experience and day-to-day work and insights that are theoretically significant and applicable.

The decision to only interview legal counsel from each jurisdiction was the urgency to capture the problem of the subject matter at its root. Notably, despite there being several market players affected by the evolving world of data privacy, they all require to consult legal practitioners to provide litigative or mitigative solutions to any challenges arising from the performance of contractual obligations, they are also, well informed to expertly highlight challenges that the public is not privy to.

3.4.2 Access and ethical issues

The subject matter of this Research study is cross-border data transfers. The primary data resources, as noted above include interviews and case studies. Notably, despite there being legislation in both jurisdictions, this being Ireland and Kenya, scholarly work reflecting an analysis of cross-border data transfers is limited on grounds of reliability. Additionally, due to the overlapping of the relationship between existing legal frameworks and technological development, many studies are rendered redundant over a brief time frame and cannot be relied on. In matters relating to ethics, every individual interviewed was contacted prior to the interview and provided consent for their data to be collected, stored and anonymized. Additionally, in accordance with the institution's ethics policies, all primary "raw" data is private and only available to the researcher.

3.5 Approach to Data Analysis

Thematic analysis will be applied to the data analysis in this investigation. Finding patterns in a data set reporting them and then examining them to ascertain their underlying importance of the steps involved. Naeem et al., (2023) posits that it involves the following 6 crucial steps:

1) Transcription and familiarization with the data alongside selection of quotations is the initial step of the thematic analysis process. This involves the creation of a transcript of data to familiarize the researcher with the responses while also facilitating an analysis of themes to select quotes representing diverse viewpoints.
2) The selection of keywords. Involves close examination of the data from interviews and allows the researcher to identify recurring patterns and develop them as a pattern.
3) Coding is the third step. This shows traces and words developed as codes and assigned segments of data to capture the data's core message, significance, and recurring themes.
4) The fourth step is the organization of codes into meaningful groups to identify patterns and relationships, thereby offering insights into the relationship developed between the research questions and research objectives.
5) The fifth step is conceptualization, which involves understanding and refining concepts emerging from the data. The researcher identifies social patterns and refines them into definitions that align with the research.
6) The last step in the thematic analysis is the development of a conceptual module. This process involves the creation of a unique data representation guided by the existing theories.

This process will be used to indicate transparency of the data collected and develop reliable outcomes, while enabling easy cross-reference of data collected through interviews.

3.6 Conclusion.

The methodologies and designs adopted for this research study have been greatly analyzed and reassessed alongside the development of this work. This has been done to ensure accuracy and transparency. The selection of these methods will ensure the results of this research study actively contribute to scholarly work that will inform cross-border data transfers on the international sphere.

4.0 Presentation and Discussion of the Findings

4.1 Overview

As highlighted in Chapter three, this section of the study was developed through employing the interpretivist philosophy alongside the desk-based comparative legal research methods which involved the selective application of the contextual integrity framework and the realist law theory to the data collected. The data was then analyzed using the thematic analysis method, allowing for shared concerns of the interviewees to be analyzed.

The primary source of data for this study was interviews with legal practitioners (attorneys from Kenya and barristers and solicitors from Ireland). This decision was informed by the need to capture recent, relevant and reliable data for presentation. The interviewee panels comprised of four individuals from both jurisdictions, with an equal number of both men and women to achieve and reflect equity, while allowing for the representation and importance of privacy from their personal perspectives. Additionally, the panels were formed with an age range of no more than twenty years between the interviewees (the youngest being twenty-five and the oldest being forty-six) as the study wanted to fully capture the realistic approach of what privacy means to individuals practicing within the time the IOT begun development in the early 2000's. This was in line with the contextual integrity framework.

Out of the intended eight interviews, seven were successful and provided the basis for the findings and presentations. Owing to the difference in cultures, ideologies, regions and practice two sets of questions were developed to suit the needs of the study, they were, however, informed by the following objectives:

1. To conduct a comprehensive comparative analysis of the data protection legislation in Ireland and Kenya, with a particular focus on the regulatory frameworks governing cross-border data transfers.
2. To assess the implications of data protection laws while identifying the specific challenges and opportunities for MNCs and regulatory bodies operating in both jurisdictions.

3. To develop recommendations for enhancing data protection practices in Ireland and Kenya, with the aim of improving best practices, cross-border security and harmonized operational efficiency.

The objectives acted as a blueprint to govern the outcome of the study.

4.2 Findings.

The results presented herein have been analyzed and measured against the concepts provided in chapter three and work to compare the legal provisions in Ireland and Kenya. The key findings are presented and broken down into three key sections guided by the objectives presented in chapter one.

4.2.1 To conduct a comprehensive comparative analysis of the data protection legislation in Ireland and Kenya, with a particular focus on the regulatory frameworks governing cross-border data transfers.

The Interviews with legal practitioners in both jurisdictions indicated that the data protection legislation provide adequate mechanisms that govern and protect data subjects' rights in as far as cross-border data transfers are involved. These provisions spell out the requirements for businesses within their respective jurisdictions and the adequacy mechanisms required to transfer data outside said jurisdictions. The check and balance systems are provided for by the Data Protection Act and various other legal instruments (both nationally and internationally) that work in harmony with respect to internationally accepted standards.

Respondents one, two, three and four, provided that this legislation was the first of its kind in Kenya. It was discussed for several years but came shortly after the introduction of the GDPR in the European Union. This legislative text was meant to govern and protect the new landscape of data privacy that was considered a toolkit for the “fourth industrial revolution.” Notably, the “young” legislation, whilst capable of providing for cross-border data transfers, remains largely ambiguous with inadequate provisions for what requirements and adequacy decisions are expected of data processors and controllers.

In contrast, interviewees five, six and seven from Ireland provided that the Data Protection Act 2018, was introduced after the Data Protection Acts 1988 and 2003, which provided adequacy mechanisms for the flow of data outside of Ireland's jurisdiction while establishing secure mechanisms for Irish data subjects. These Acts were guided by a larger framework of EU legislation that governed free flow of data within the EEA, and stricter provisions were enforced upon the consideration of growing concerns across the globe, resulting in the EU parliament introducing the GDPR which naturally took effect in all member states, including Ireland.

In spite of this, both Ireland and Kenya find themselves at odds with the enforceability of the laws, given that despite the provisions existing and indicating a clear course of action, the regulatory bodies in each country cannot fully ensure that MNCs operating in their respective jurisdictions are compliant with the laws, and are also held accountable in the event of breaking said laws. The endeavor is not so bureaucratic as it is more political with severe consequences for both the parties involved in litigation in the event of breaking the law.

4.2.2 To assess the implications of these data protection laws while identifying the specific challenges and opportunities for MNCs and regulatory bodies operating in both jurisdictions.

The findings of this objective revealed the inextricable codependency of MNCs, the respective governments of both countries and the regulatory authority bodies that monitor market player compliance. It indicated that while data privacy for data subjects is paramount, there are other variables that have influence over how effective regulatory action is. Interviewees five, six and seven argued that the GDPR remains the international standard that governs data protection and as such it is paramount for parties operating within Ireland to adhere to the provisions of both the 2018 Act and the GDPR. In addition to this, interviewee six presented that whilst these laws exist, Ireland is a country that still relies on foreign direct investment to a certain extent and as such, it continues to find a balance between enforcing the law and maintaining a relationship with the multinational corporations operating within the jurisdiction.

Arguably, large technology organizations operating in Ireland, generate revenue upward of hundreds of millions, these figures are a fraction of what the government earns from these companies and does not account for the pharmaceutical companies and other e-commerce platforms that also have subsidiaries in the state. As a result, the government recommends that

whilst the data protection laws are stringent, they also provide room for the development of best practice and the introduction of transfer mechanisms i.e., standard contractual clauses (SCCs), that allow for the continuity of business operations even in the wake of violation of laws as seen in the Shrems I and II cases.

In comparison, interviewees three and four had clashing opinions on the subject matter of this objective. Interviewee three argued that Kenya is a third-world country, and it is essential not to conflate meeting international standards with being "a global player." While Kenya needs multinational corporations operating within its jurisdictions, it is not applicable the other way around. They added that the culture of privacy is also not "inherently important for Kenyans" and it would be wise not to penalize multinationals in the market. Interviewee four provided that the new legislation was vital as it finally gave the legal body in Kenya the capacity to protect data subjects and the state from predatory and malicious practices by international organizations, more so those within the financial and technological space, who constantly violated privacy and went as far as accessing data subjects' contact logs to send defamatory messages as an incentive for quicker activity from their clients.

Notably, the responses gathered during the study highlight the importance of both parties (the MNCs and regulatory authorities) to work together, as it establishes an environment for both to develop best practice in lieu of a more expensive and longer process of penalizing market players for misconduct and litigation which in turn takes a longer time and affects shareholder value of MNCs involved. Additionally, the governments remain silent players, that control the parties involved.

4.2.3 To develop recommendations for enhancing data protection practices in Ireland and Kenya, with the aim of improving best practice, cross-border security and harmonized operational efficiency.

This section of study found that, despite there being clear regulatory provisions i.e., data protection legislation, data protection practices are contingent on multiple factors. These factors are:

1) The introduction of incentivized compliance and enforcement mechanisms. Interviewee seven argued that the introduction of new policies would allow certain subsidiaries to have

DPA-approved activities in the state, which in turn would enhance shareholder confidence and result in better market presence. This would have a ripple effect to ensure that the businesses able to meet this threshold have a bigger advantage in comparison to those that cannot meet these requirements.

2) The promotion of research and innovation in data security mechanisms to counter the quickly developing and often unregulated new technology released. All interviewees, highlighted the need to have in-house personnel trained and up to date with ongoing developments in the international space, including the education of the personnel by cyber security specialists, who would ensure the regulatory bodies are at the forefront of privacy concerns.
3) Through raising awareness on data privacy, which can be achieved through mass education and forums. This facilitates IT professionals, legal practitioners and the relevant regulatory authority to attend training events that certify them as recognized data protection personnel, with keen understanding of incident response management, emerging data security challenges and digital literacy.

The implementation of these factors would greatly enhance the ability of the parties involved to ensure data security.

4.3 Discussions.

The construction of the theoretical frameworks that guided this research's conclusions were developed in chapters two and three. The theories and ideas drawn from existing literature will also be discussed in this section of the paper, to bring focus on how they merged and provided a better understanding of cross-border data transfers and MNCs regulatory compliance.

4.3.1 Technology-Based Governance of Cross-Border Data Transfers

Technological capability is crucial in ensuring data protection effectiveness and facilitating adequacy approved cross-border transfers. As such, there is a growing importance to ensure that governments allocate adequate resources to achieve this goal. Notably, while it reads well on paper it is extremely difficult to maintain the regulation of constant technological advancement, more so as governments have budgetary requirements and constraints despite them being expected to

compete with multi-billion conglomerates, whose business models are cutting edge technological products and services.

Ireland is recognized as a well-established technology hub in the EEA with a robust digital economy. It is the EU headquarters of Google, Meta and Microsoft, some of the world's largest technology companies. Interviewee Seven states that Ireland has a sophisticated cybersecurity framework, which has resulted in the development of large data centres, comprehensive cybersecurity strategies and infrastructural support to ensure the best market service delivery and protection. That be as it may, the interviewee also noted that the DPO lacks the same infrastructural resources and that, despite the improvement, there is still significant room for development and operations to ensure the workload is met.

Similarly in Kenya, there is a great disconnect between the provisions of the law and the technological infrastructure provided for the performance of the regulatory authority body. There is also a further challenge as there is a fragmentation and overlap between the task forces deployed to mitigate any challenges arising from noncompliance. Interviewees two and four, argue that Kenya’s technology backdrop is at its nascent stage, making it difficult to attain the innovative technology that is available for wealthier global market players. Interviewee one, delivered a stronger emphasis on the influence of foreign players in the country, mentioning the most recent country wide strike against a finance bill that was introduced by the World Bank in Kenya, which upon closer inspection indicated insidious clauses providing for the syphoning of data, deregulation of cross-border data transfers and covert surveillance activity through banks and mobile transactions. The state lacks the resources to introduce better technology, and as such its reliance on foreign aid to achieve such goals has led to the violation of data privacy law.

In summary, while performing as best as they can with the allocated resources, both territories could benefit from improved technology infrastructure. This cannot be realistically achieved in a short time frame, and as such, it is more practical to ensure that regulatory action in the form of penalizing non-compliant players is employed. This will provide capital from fines that may be used to invest in better technology infrastructure.

4.3.2 Enforceability of Data Protection Law

To establish a system that guarantees data protection and effective cross-border data transfers by extension, it is imperative to have data protection law enforcement mechanisms. Notably, this emphasizes the relationship between legislation and the critical individuals tasked with regulatory power over data protection: the Data Protection Commission and the Office of the Data Protection Commissioner for Ireland and Kenya, respectively. These offices must be independent of government interference and any scrutinous action by the countries they serve save for audit purposes, unfortunately this is not the case.

The Kenyan Data Protection landscape is governed by the DPA 2019, this legislation came into effect a year after the GDPR took effect in the European Union, notably, it is a not as mature. In this light, it is important to indicate the DPA 2019, strongly borrowed from the GDPR in both performance and text, however, these two legislations are extremely different in their provisions and performance mechanisms. Interviewee four, notes that the DPA 2019, lacks comprehensiveness while addressing adequacy requirements for cross-border data transfers and stipulations for MNCs operating within the Kenyan landscape, often failing to address the legal requirements for contractual performance and compliance for companies with a significant market presence, without a physical presence in the country, and what happens in the event of non-compliance. Additionally, interviewees one and two highlight that while the ODPC oversees regulatory governance, it is an office that is still developing and is riddled with budgetary constraints that not only inhibit the performance of the office but leave it vulnerable to outsider influence. Most importantly, interviewee three highlights that the office chair has a long history of illegal infractions and makes their performance in their role questionable on the grounds of integrity and probity.

The Irish data protection landscape is governed by the GDPR and the DPA 2018, two stringent legislations in their enforcement mechanisms. The primary organ in charge of overseeing regulatory compliance is the Data Protection Commission. Interviewee six notes that the DPC is well suited to conduct audits, penalize non-compliance, and suspend data processing activities, which have been observed in flagship cases such as Shrems I and II. It is, however, a point of concern that the DPC is overworked with above-average caseloads while having a small employee base. The interviewee notes that the former chair of the DPC declined to have new roles introduced to enhance delivery on their team, and this action had a ripple effect and led to mediocre

performance and longer than average periods to impose fines and penalize non-compliance. That be as it may, Interviewee seven believes that the DPC is now well staffed and is delivering better in comparison to the year 2021, after the government introduced new dockets, as the former structure was unsustainable and unfit for its purposes. As such, this action led to improved enforcement.

As evidenced, this study recognizes the need for enhanced effectiveness of enforcement mechanisms, and that a more capital and resource intensive approach guarantees better compliance of MNCs alongside more action from regulatory authorities. This may be achieved through increasing resources for Data Protection Authorities both through human resource and funding, independence from the government only and only allowing so in dire circumstances for both Ireland and Kenya and finally, developing a more detailed monitoring system and legal stipulations for Kenya.

4.3.3 Existing Mechanisms and Barriers to Adequacy

Multinational corporations rely on data flows internationally, a result of digitization, e-commerce, and globalization. Cross-border data transfers are a product of data movement across multiple jurisdictions with varying adequacy mechanisms. Data protection authorities are tasked with ensuring these transfers are compliant with data protection laws to ensure that data subjects and information relating to them are safeguarded in accordance with the highest possible standards. Interviewee one, presents that human beings are the weakest link in cyber security, as they are subject to biases and external pressures that machinery is exempt of, and herein lies the challenge for efficient mechanisms and factors that overlap adequacy and in turn become barriers to cross-border data transfers.

Adequately captured in previous arguments, Ireland being part of the European Union, has internationally regarded and mechanisms in place. The jurisdiction follows the provisions of the GDPR in matters concerning cross-border data transfers, these are considered transfers to a third country outside the EU. The GDPR provides that, if the European Commission can determine that a country offers an adequate level of data protection i.e., Japan and Switzerland, it is permissible to allow free flow of data to such a jurisdiction. Additionally, in the event of an adequacy decision being absent, standard contractual clauses are the best alternative to ensure that data transfers can

occur, these clauses are pre-approved legal agreements that bind both data importers and exporters to the provisions of the GDPR. Interviewee five, highlights that this is what the United States of America (the EU's largest market) has applied for easy cross-border data transfers. Interviewee Six explains that the former two are the most regarded approaches to facilitate data transfers, however, binding corporate rules and derogations are permissible.

Ireland being a technology hub, has ensured effectiveness of the existing mechanisms, nonetheless, interviewees five and seven acknowledge that establishing Standard contractual clauses and binding corporate rules is an arduous and expensive task, that requires relentless monitoring of legal compliance of MNCs, something that given the history of the Irish data landscape is subject to failure.

The results in Kenya paint a significant contrast, especially as the Data Protection Act 2019 is unclear in matters relating to cross-border data transfers. This area of the law is vague, and its interpretation is subject to performance bias, which exposes data subjects to violations of their rights. Interviewee one notes that the DPA 2019 requires data transfers to only occur when adequate levels of protection are met, this leads to the question of "whose adequate levels" are being referred to. If it is the GDPR's adequacy approval, Kenya itself does not meet the requirements as a state, considering it lacks the technology and security infrastructure to ensure data subjects' privacy is maintained and, in this light, Kenya as a state, therefore cannot provide clarity in its own law for a threshold to be met. Interviewee one adds that, in addition to this, a transfer may be approved in the event a data subject explicitly consents to the transfer for the performance of a contract and "other legitimate grounds" which is more ambiguous than the requirement.

That be as it may, the Office of the Data Protection Commissioner has the mandate to require organizations to conduct data protection impact assessments before transferring data outside Kenya, this preemptive approach coerces MNCs to comply and prove existing protective safeguards. In addition, the state now requires for MNCs to also register their operation in Kenya with them to avoid the moratorium for businesses in Kenya, established to curb noncompliance.

This section of the study highlights the need for both Irish and Kenyan businesses to introduce more stringent mechanisms to enhance compliance, more so in Kenya, as the law needs to be

revised to effectively capture the need of data subjects' rights and for more efficient data privacy laws.

4.3.4 Socio-cultural and Economic factors Influencing Compliance, Enforcement and Legislation

This section of the study is influenced by H.L.A Hart's legal positivism theory as discussed in chapter three. Hart's theory is separated by three different perspectives, in this section the first perspective is applied, and it provides that: 'understanding legislation from the standpoint of those who must abide by the rules is important, because it highlights how people learn to embrace and interpret the laws.' Notably, laws in each jurisdiction are influenced by cultures and traditions, socially accepted norms, and economic practices, these are variables that played a crucial role in the adherence, implementation, and perception of data privacy laws in Ireland and Kenya, and this has influenced the operation of MNCs.

An analysis of the data collected, highlights the importance of a strong economy in Ireland, this is observed in its efforts to diversify its economic and political policies to attract foreign investment from MNCs. Interviewee seven highlights that the Irish government has made significant investment towards innovation of data security, especially considering the number of 'tech' players in the market who consistently provide a source of revenue to the country and also due to the fact that Ireland is known for being a technology hub in the Western hemisphere of Europe. Consequently, to meet market demands, businesses operating in Ireland invest in compliance mechanisms to meet market demands, which often presents as the training and hiring of Data Protection Officers.

From a socio-cultural perspective, there is a longstanding history of data privacy rights and human rights not only in Ireland but across the EU. This is observed in the revisions of the data protection acts and the introduction of the GDPR, whose purpose was to guarantee data subjects rights and integrity of data across borders. Interviewee six highlights the growing concerns among legal practitioners towards the performance of the Data Protection Commision, especially the laxity in pursuing penalties, given that there is an expectation for the office to ensure regulatory compliance. This results from a culture of accountability in the Irish population, more so towards the government and state offices.

The study also discovered the impact of economic and socio-cultural factors influencing compliance, enforcement, and legislation in Kenya. As discussed above, the Kenyan population has varying responses to the new data privacy landscape, this is keenly observed from the nature of cases the office of the Data Protection Commissioner handles, most of which are vexatious in nature. Interviewees one, two, three and four provided the Act is foreign, and the socio-cultural approach is divorced from the provisions. While the citizens of Kenya are aware of their rights and their constitutional mandate to privacy, a great majority do not view data privacy at large as an ongoing concern, time and again, this sentiment has changed in the wake of national scandals i.e., Cambridge Analytica, however, upon the passing of scandals the citizenry remains impassive to the specific law. This is also driven by the mistrust of governmental influence over data privacy systems, as they are regularly broken to enforce "extrajudicial punishment" for citizens considered a threat to the government.

A closer analysis of the economic influence indicates a sharper contrast between what the citizens believe to be a pressing developing country's needs and "first-world problems," where the subject matter is involved. Interviewee four, who actively works with financial institutions, expressively indicated that the population is more concerned with the dire economic state of the country, and as such establishing data protection mechanisms within their businesses, much less with multinational corporations is a non-issue. The larger population cannot afford to establish adequacy mechanisms or pursue regulatory non-compliance by MNCs. While this argument is founded, two truths can coexist, Kenya is also considered the silicon savannah, a champion of a digital and mobile economy particularly in the financial sector, with M-Pesa being the first system in Africa to facilitate exchange of money over vast landscapes, without the involvement of financial institutions. This system is still unable to fully guarantee data subject privacy due to governmental interference.

In conclusion, both jurisdictions experience advantages and disadvantages at extreme polar ends, when the economic and socio-cultural influences are scrutinized. Ireland benefits from a long history of privacy mechanisms and faces challenges in resource allocation, while Kenya is considered a benchmark for data privacy on the African landscape and has a long more ground to cover in regard to cultural adaptation and lack of resources.

4.3.5 Harmonization and Alignment of Regulations

The analysis and exploration of theories and frameworks developed in this research indicate that there is a need for Kenya as a state to revisit its legislation, young as it may be. Notably, this has been presented by the interviews conducted with the Kenyan panel, the findings are that despite there being incentive to take emboldened steps towards being among the first countries in Africa to introduce data privacy laws, the laws need to be revised in order to reduce legal ambiguity and establish more integrity to the framework, disallowing the interference of the government and the capacity for MNCs to override the legislation in general.

Kenya's Data Protection Act 2019 lacks adequate mechanisms to facilitate uncompromised cross-border data transfers within the global market, and while this is a disadvantage, it is also an opportunity for the country to enhance the provisions within the DPA 2019, to introduce reestablish itself as a committed international player. This may be achieved through mirroring the GDPR, in a practical manner to facilitate the country's current standing. Best captured, interviewee four provided that legal definitions around consent, data processing and cross-border transfer mechanisms (adequacy) must be re-written, allowing for more control by data subjects and the introduction of a recommended application of standard contractual clauses and binding contractual clauses, which would require MNCs and any other data controllers and processors involved in any data flow activity outside Kenya, to invest more time and finances allowing for the ODPC to generate revenue for infrastructural development. Not only would this improve the country's image internationally, but it would also apply a similar level of GDPR stringency, that would harmonize the two laws.

This process would require international consulting and evaluation of outcomes. Interviewee one, who had a work trip in New Zealand, indicated the state achieved a successful process of the harmonization. They provided, that in 2020 New Zealand revised her Data Privacy Act to mirror and achieve harmony with the GDPR, a process which resulted in enhanced protection of data subject's rights, more efficient data breach notifications and mitigative actions in the wake of a breach and stronger enforcement mechanisms to buffer out noncompliance. Verily, New Zealand achieved international recognition resulting in increased trust and competitiveness in the international market, more so for technology companies, the transfer of data from the country to

the EU without any additional legal safeguards and enhanced data governance and cybersecurity practices within the state.

Kenya does not have the spending power New Zealand has, as evidenced by the published budgetary allocation by both states, it does, however, can leverage public and private partnerships to facilitate capacity building. This action will play a critical role in adequately educating the public on the need for a compliance culture in the state. The ripple effect allows the citizens as stakeholders in their digital economy, to demand compliance by market players. The state would also employ diplomatic engagement with the EU, especially to work with the European Data Protection Board to facilitate training and funding to reach adequacy standards, while boosting multilateral trading activity where both parties benefit.

To summarize, Kenya, if willing to leverage adversity, will experience long-term benefits. The state will be better suited within the African landscape to facilitate digital trade and innovation through cross-border transfers, to first-world countries without additional legal requirements and the state will also gain competitive edge for the Kenyan market, making it an EU destination for foreign direct investment, without the additional concern of setting up standard contractual clauses or binding corporate rules to facilitate data subject privacy and data flows.

4.4 Conclusion

As highlighted in the findings and discussions above, the comparative analysis of data protection legislation facilitating cross-border data transfers in Ireland and Kenya, has provided a stark contrast between the states. It is paramount to acknowledge that unlike Kenya, Irland has had data protection mechanisms and legislation for over thirty-five years, a period during which, revisions of the laws have been made to buffer out potential threats to the state. Additionally, Ireland is a member of the European Union and as such has a leveraged position for security and access to resources that is provided by this proximity. Kenya, on the other hand, is an African state that has taken incentive to provide adequate mechanisms and seeks to be recognized as an international player. The diligent act of enacting data privacy laws, a foreign, yet important piece of legislation is not only important for the state to participate in the “fourth industrial revolution," but it is also a means to gaining international recognition as a capable country.

In conclusion, this study has established that the data protection legislation in the Kenya is riddled with legal ambiguity, and as such, limits the enforceability of the law and full participation in legally protected cross-border transfers. The study has also discovered that the challenge not only lies with the legislation, but the independence of the office of the Data Protection Commissioner alongside, political interference by the government of Kenya and other offices with instruments to override the legislation. Furthermore, the study has also discovered existing challenges in the enforceability mechanisms in Ireland, this is observed by the inability to effectively handle, investigate and audit businesses with operation in the state, while also handling the caseloads in the Data Protection Commission office. This has resulted in the slowed and potentially ignored penalization of MNCs noncompliance in matters involving inadequate data protection, which extends to insecure data subject privacy during cross-border data transfers.

5. Concluding Thoughts on Research Contribution, Its Limitations, Recommendations and Suggestions for Further Research.

5.1 Implications of Findings for the Research Questions.

The study's findings were driven by the questions and objectives developed at the onset of the research. They were developed after an initial analysis of the data protection landscape in both Ireland and Kenya and a critique of the existing literature by academics, legal practitioners, researchers, and scholars in the fields of business, law, and technology with an emphasis on data privacy protection and cross-border data transfers. Notably, two sets of interview questions were developed to guide the inquiries, considering each jurisdiction has different laws and varying regulatory compliance challenges. As such, all findings required further inquisition based on the expertise of the interviewees.

The findings proved reliable and provided results absent from existing literature. The respondents expressed in detail factors influencing and affecting cross-border data transfers, data protection legislation, enforcement mechanisms and problems within the data protection landscape. These findings probed more questions on what other influences exist outside the limited control of data controllers, processors, legal representatives, and even multinational corporations, this provided data that was used to present the results of this research study.

Notably, the questions posed during this research demanded accountability and probity from the respondents. The responses were sensitive, and in four out of the seven successful interviews, the interviewees paused to ensure that their identities and remarks would not be publicized, as this would negatively affect their careers. Four out of the seven were from a similar jurisdiction. In conclusion, all the findings from this study influenced the presentation of this research study.

5.2 Contributions and Limitations of the Research

The findings and the contributions of the literature review in this study have proven that there are challenges within the data privacy landscape. The chosen jurisdictions in this research were Ireland and Kenya; arguably the two states are on two different continents and are governed by extremely different policies, that be as it may, they are both common law jurisdictions, and the common denominator in their data privacy landscape is the GDPR. This study facilitated an inquiry into

what makes the commonalities present opposite impacts on the countries and their facilitation of cross-border data transfers. The study has established that, despite there being existing frameworks and mechanisms to govern the use and protection of data and data subject's rights, there are outliers whose nature are economic, political, socio-cultural, and technological that have adverse effects on the impact of how these curated systems and laws work in harmony and more often, their disharmony. This study has also provided a current analysis of the limitations of data privacy. It is often suggested that technology is the problem, however, the data collected has proven that it is, in fact, the individuals involved in facilitating data flows, enforcing the law, and guaranteeing security that are the bane of the challenges.

The main limitation of this study was the limited quantity of existing literature analyzing the data privacy frameworks in Kenya. Most of the literature available on the Kenyan Data Protection Act 2019, was geared towards a comparative analysis of other Acts within the African landscape and the assessment of its integrity in the e-commerce landscape in Kenya, while those in Ireland did not feature a critique on cross-border data transfers outside the European Economic Area and the United States of America. Additionally, it was challenging to source reliable and honest interviewees willing to discuss the privacy landscape in Kenya, especially as the third quarter of the year 2024 was driven by political dishevel. Outside these factors, there may be relative bias on the side of respondents that influenced the outcome of this research.

5.3 Recommendations for Future Research.

This research has provided insight into the ongoing challenges within the data privacy landscape in the Irish and Kenyan jurisdictions. It has adequately captured, through its comparative analysis, how cross-border transfers are affected by the existing legal frameworks. The findings have proven key areas, presented as frameworks, which are the harmonization and alignment of regulations, the technology-based governance of cross-border data transfers, the enforceability of data protection laws, the existing mechanisms and barriers to trade and the socio-cultural and economic factors influencing compliance, enforcement, and legislation. These frameworks can be used as toolkits to develop improved and more coherent data privacy mechanisms that ease cross-border data transfers.

Future research may use this study as a benchmark to assess the development of best practice, development of technological infrastructure, the assessment of the revision of former legislation (in this case the Data Privacy Act 2018 and 2019 for Ireland and Kenya respectively), the assessment of harmonization of laws and mechanisms and the impact of compliance (or noncompliance) in both jurisdictions.

5.4 Final Conclusion and Reflections

This study set out to explore the comparative analysis of data protection legislation in Ireland and Kenya while specifically providing for cross-border data transfers. The research findings identified critical areas of concern, and discussions on how to mitigate these challenges were presented. The implications of this comparative analysis offer insight not only into Ireland and Kenya but also into how the data privacy landscape affects other countries, given the varying capacity to allocate resources and meet international standards. This facilitates discussions on data flows, global data governance and striking a balance between digital sovereignty and data protection compliance.

In hindsight, upon reflecting on the research process, this study has brought to light the overlapping nature and concerning speed at which technology is developed and surpasses the implementation of the law, this highlights the need for digital governance to operate at an equally fast pace to control technology and cybersecurity challenges. Additionally, this research study has also significantly emphasized the need for effective policy development within the international arena, an action that will be used to ensure that technology will not be used as an instrument to further wedge economic disparity, especially against developing countries, whose digital sovereignty is contingent on compliance of multinational corporations and other international agents.

REFERENCES

African Union, (2014) *African Union Convention on Cyber Security and Personal Data Protection*. Available at: https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf [Accessed 22 July 2024].

Babalola, O., (2024) Transborder flow of personal data (TDF) in Africa: Stocktaking the ills and gains of a divergently regulated business mechanism. *Journal Name*, [online] Available at: https://www.sciencedirect.com/science/article/pii/S0267364924000074 [Accessed 22 July 2024].

Belli, L., Lorenzon, L., Fergus, L. and Britto, W., (2020) *The Brazilian General Data Protection Law (LGPD): Introduction to LGPD and Unofficial Translation*. CyberBRICS Project at FGV Law School. Available at: https://cyberbrics.info/wp-content/uploads/2020/03/The-Brazilian-LGPD [Accessed 24 July 2024].

Bongiovi, J.R., (2019) Review of *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, by S. Zuboff. *Social Forces*, 98(2), pp.6-11. Available at: https://www.jstor.org/stable/26862460 [Accessed 20 July 2024].

Bowmans, (2019) *Snapshot Analysis of the Data Protection Act 2019*. Available at: https://bowmanslaw.com/insights/snapshot-analysis-of-the-data-protection-act-2019/ [Accessed 23 July 2024].

Bradford, A. (2012) 'The Brussels Effect', *Northwestern University Law Review*, 107(1), pp. 19-35. Available at: https://scholarlycommons.law.northwestern.edu/nulr/vol107/iss1/1 (Accessed: 29 July 2024).

Case C-311/18, *Data Protection Commissioner v Facebook Ireland Ltd, Maximilian Schrems*, request for a preliminary ruling under Article 267 TFEU from the High Court (Ireland), made by decision of 4 May 2018, received at the Court on 9 May 2018.

Case C-362/14, *Maximillian Schrems v Data Protection Commissioner*, joined party: Digital Rights Ireland Ltd., request for a preliminary ruling under Article 267 TFEU from the High Court (Ireland), made by decision of 17 July 2014, received at the Court on 25 July 2014.

Chander, A. and Schwartz, P.M. (2023) 'Privacy and/or trade', *The University of Chicago Law Review*, 90(1), pp. 60-71. Available at: https://paulschwartz.net/wp-content/uploads/2023/01/Chander_Schwartz-Privacy-and-or-Trade-Chicago-Law-Rev-2023.pdf (Accessed: 18 June 2024).

Chugh, U., (2023) The evolution of privacy laws in the digital age: Challenges and solutions. *Indian Journal of Law*, 1, pp.51-60. Available at: https://doi.org/10.36676/ijl.2023-v1i1-07 [Accessed 20 July 2024].

Consumer Protection Act, No. 46 of (2012) Date of Assent: 13thDecember 2012.

Court of Justice of the European Union, (2018) *Judgment of the Court (Grand Chamber) of 24 September 2019 – Google LLC v CNIL*. Case C-311/18. [online] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62018CJ0311 [Accessed 26 July 2024].

Data Protection Act 2018 Explanatory Memorandum, (2018) Available at: https://www.gov.ie/pdf/?file=https://assets.gov.ie/122559 [Accessed 25 July 2024].

Data Protection Act, No. 24 of 2019, Subsidiary Legislation.

Data Protection Act, Chapter 411C, Revised Edition 2022.

Dickhaut, E., Janson, A., Söllner, M. and Leimeister, J.M., 2023. Lawfulness by design – development and evaluation of lawful design patterns to consider legal requirements. *European Journal of Information Systems*, pp.1-28.

Ethics & Compliance Initiative, (2021) *Ethics and Compliance in Multinational Organizations*. Available at: https://www.ethics.org/wp-content/uploads/2021-ECI-WP-Ethics-Compliance-Mulinational-Organizations.pdf [Accessed 10 July 2024].

European Commission, (2003) *Internal Market, Industry, Entrepreneurship and SMEs*. Available at: https://commission.europa.eu/about-european-commission/departments-and-executive-agencies/internal-market-industry-entrepreneurship-and-smes_en [Accessed 14 July 2024].

European Commission, (2003) *First report on the implementation of the Data Protection Directive (95/46/EC). Report from the Commission. COM (2003) 265 final, 15 May 2003*. Available at: http://aei.pitt.edu/45392/1/COM_(2003)_265_final.pdf [Accessed 24 July 2024].

European Data Protection Board, n.d. *European Data Protection Board: Who We Are*. [online] Available at: https://www.edpb.europa.eu/about-edpb/who-we-are/european-data-protection-board_en [Accessed 16 July 2024].

European Data Protection Board, (2021) *Guidelines 05/2021 on the Interplay between the Application of Article 3 and the Provisions on International Transfers as per Chapter V of the GDPR*. [online] Available at: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052021-interplay-between-application-article-3_en [Accessed 17 July 2024].

European Parliament and Council, 1995. *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals regarding the processing of personal data and on the free movement of such data.* Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046 [Accessed 10 July 2024].

European Union, (2012) *Charter of Fundamental Rights of the European Union*. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012P%2FTXT [Accessed 10 July 2024].

EUR-Lex, (2009) *The Treaty of Lisbon*. Available at: https://eur-lex.europa.eu/EN/legal-content/summary/the-treaty-of-lisbon.html [Accessed 14 July 2024].

FRA (European Union Agency for Fundamental Rights), (2009) *Treaty on the Functioning of the European Union: Article 16 (ex-Article 286 TEC)*. Available at: https://fra.europa.eu/en/law-reference/treaty-functioning-european-union-article-16-ex-article-286-tec [Accessed 10 July 2024].

FRA (European Union Agency for Fundamental Rights), (2024) Article 8 - Protection of personal data. Available at: https://staging.fra.europa.eu/en/eu-charter/article/8-protection-personal-data [Accessed 10 July 2024].

Gamble, A., (2013) Economic libertarianism. In: M. Freeden and M. Stears, eds. *The Oxford Handbook of Political Ideologies*. Online edn, Oxford Academic, 16 Dec. 2013. Available at: https://doi.org/10.1093/oxfordhb/9780199585977.013.0008 [Accessed 10 July 2024].

GDPR (2018) *Article 44: General principle for transfers.* Available at: https://gdpr.eu/article-44-transfer-of-personal-data/ (Accessed: 19 July 2024).

GDPR (2018) *Article 45: General principle for transfers.* Available at: https://gdpr.eu/article-44-transfer-of-personal-data/ (Accessed: 19 July 2024).

Gellman, R. (2014) 'Fair Information Practices: A Basic History', *SSRN Electronic Journal*. Available at: http://dx.doi.org/10.2139/ssrn.2415020 (Accessed: 18 June 2024).

Gichuhi, P., (2020) The Data Protection Act 2019: A new dawn for privacy in Kenya. *Kenya Law Review*, 12(1), pp.45-60.

Gitari, S.M. (2020) *Reforming the institutional and legal frameworks of E-commerce in Kenya: consumer rights protection in the digital economy*. Strathmore Law School, Strathmore University.

Ginosar, A., (2014) Public-Interest Institutionalism: A Positive Perspective on Regulation. *Administration & Society*, 46(3), pp.301-317. Available at: https://doi.org/10.1177/0095399712453926 [Accessed 10 July 2024].

Greenleaf, G., (2020) *Evaluating GDPR: Global Impact on Surveillance Practices*. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3635118 [Accessed 13 July 2024].

G20 (2019) 'G20 Osaka Leaders' Declaration'. Available at: www.consilium.europa.eu/media/40124/final_g20_osaka_leaders_declaration.pdf (Accessed: 18 June 2024).

International Trade Administration (2017) *EU-U.S. Privacy Shield Framework*. Available at: https://www.privacyshield.gov/ps/eu-us-framework (Accessed: 29 July 2024).

Kelleher, D., 2020. GDPR in Ireland: The role of the Data Protection Commission. *Irish Journal of European Law*, 23(1), pp.10-25.

Kenya Constitution, (2010) Available at: https://www.kenyalaw.org/lex/rest/db/kenyalex/Kenya/Legislation/English/Constitutions/Constit

ution%20of%20Kenya%20%28Rev.%202010%29/docs/ConstitutionofKenya2010.pdf [Accessed 15 July 2024].

Kenya Gazette Supplement No. 236, (2021) *The Data Protection (General) Regulations, 2021*. Available at: https://www.odpc.go.ke/wp-content/uploads/2024/03/THE-DATA-PROTECTION-GENERAL-REGULATIONS-2021 [Accessed 15 July 2024].

Kenya Law Reform Commission, (2010) *Constitution of Kenya - Article 31: Privacy*. Available at: https://klrc.go.ke/index.php/constitution-of-kenya/112-chapter-four-the-bill-of-rights/part-2-rights-and-fundamental-freedoms/197-31-privacy [Accessed 13 July 2024].

Kenyatta, U. (2019) *Speech by His Excellency Hon. Uhuru Kenyatta, C.G.H., President of the Republic of Kenya and Commander in Chief of the Defence Forces during the 2019 State of the Nation Address at Parliament Buildings, Nairobi*. Available at: https://www.un.int/kenya/statements_speeches/speech-his-excellency-hon-uhuru-kenyatta-cgh-president-republic-kenya (Accessed: 25 July 2024).

Khan, R.A., Khan, S.U., Akbar, M.A. and Alzahrani, M., (2022) Security risks of global software development life cycle: Industry practitioner's perspective. *Journal of Software: Evolution and Process*. First published 23 November 2022. Available at: https://doi.org/10.1002/smr.2521 [Accessed 10 July 2024].

King'ori, M., (2024) Towards a continental approach to data protection in Africa: Perspectives from privacy and data protection harmonization efforts in Africa. Future of Privacy Forum (FPF), February.

King'ori, M. (2021) *Kenyan High Court (temporarily) struck down the national digital ID Card*. Future of Privacy Forum (FPF), 14 January.

Kuner, C., (2019) The Internet and the global reach of EU law. In: M. Cremona and J. Scott, eds. *EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law*. Oxford: Oxford University Press, pp. 112-145.

Kuner, C., Bygrave, L., Docksey, C., Drechsler, L., Hijmans, H., Kranenborg, H., Svantesson, D., Tosoni, L., Terwangne, C., Kotschy, W., Kosta, E., Georgieva, L., Polčák, R., Zanfir-Fortuna, G., González Fuster, G., Lynskey, O., Moore, D., Millard, C., Kamarinou, D. and Oliveira, P. (2020) *The EU General Data Protection Regulation (GDPR): A Commentary*. Available at: https://doi.org/10.1093/oso/9780198826491.001.0001 (Accessed: 18 June 2024).

Iakovleva, S., (2022) On Digital Sovereignty, New European Data Rules, and the Future of Free Data Flows. *Legal Issues of Economic Integration*, 49(4), pp.339-348. Available at: https://hdl.handle.net/11245.1/8fbaee27-8e27-499f-b6ab-d5f764e904a3 [Accessed 16 July. 2024]

Legal Theory (2000) 'Title of the Article,' Legal Theory, 6(2), pp. 127–170. Doi: https://doi.org/10.1017/S1352325200062017.

Li, H., Yu, L. and He, W., (2019) The impact of GDPR on global technology development. *Journal of Global Information Technology Management*, 22(1), pp.1-6. Available at: https://doi.org/10.1080/1097198X.2019.1569186 [Accessed 24 July 2024].

Murphy, M., (2020) The enforcement challenge: Ireland's Data Protection Commission and GDPR compliance. *Journal of Internet Law*, 23(8), pp.3-10.

Mweu, N., (2022) *Kenya - Data Protection*. Available at: https://www.dataguidance.com/notes/kenya-data-protection [Accessed 15 July 2024].

Muturi, J. (2023) *Probe into Worldcoin's unauthorized data collection from Kenyans*. Available at: http://www.parliament.go.ke/ (Accessed: 1 August).

Naeem, M., Ozuem, W., Howell, K., & Ranfagni, S. (2023). A step-by-step process of thematic analysis to develop a conceptual model in qualitative research. *International Journal of Qualitative Methods, 22*. https://doi.org/10.1177/16094069231205789

Nissenbaum, H. (2009) *Privacy in context: Technology, policy, and the integrity of social life.* Stanford: Stanford University Press.

Nyaga, A. (2023) *Data privacy & vicarious liability: The ODPC finds Safaricom PLC not liable for data breach by its employee.* Available at: https://fmcadvocates.com/wp-content/uploads/2023/10/Case-Brief-Vicarious-Liability-Data-Privacy-Alfred-Nyaga-and-Vanessa-Mugo-18.10.2023.pdf (Accessed: 10 August 2024).

Obaidat, M.A., Obeidat, S., Holst, J., Al Hayajneh, A. and Brown, J., 2(020) A comprehensive and systematic survey on the Internet of Things: Security and privacy challenges, security frameworks, enabling technologies, threats, vulnerabilities, and countermeasures. *Computers*, 9(2), p.44. Available at: https://doi.org/10.3390/computers9020044 [Accessed 10 July 2024].

OECD (1999) *Guidelines for Consumer Protection in the Context of Electronic Commerce*. Available at: https://www.oecd-ilibrary.org/governance/guidelines-for-consumer-protection-in-the-context-of-electronic-commerce_9789264081109-en-fr (Accessed: 1 August 2024).

Office of the Data Protection Commissioner, (2022) *Office of the Data Protection Commissioner Kenya*. Available at: https://www.odpc.go.ke/ [Accessed 15 July 2024].

O'Hara, K., (2019) National security and data protection in Ireland: A critical analysis of the Data Protection Act 2018. *European Human Rights Law Review*, 4, pp.370-382.

Privacy International (2018) *Further questions on Cambridge Analytica's involvement in the 2017 Kenyan Elections and Privacy International's investigations*. Available at: https://privacyinternational.org/ [Accessed 25 July 2024).

Ruggie, J., (2017) International regimes, transactions, and change: embedded liberalism in the postwar economic order, pp.133-170. Available at: https://doi.org/10.4324/9781315251981-6 [Accessed 10 July 2024].

Saunders, M., Lewis, P., & Thornhill, A. (2012) Research methods for business students. Pearson

Saunders, M., Lewis, P. and Thornhill, A. (2015) 'Understanding Research Philosophies and Approaches'. Research Methods for Business Students, 4, pp. 106–135.

Saunders, M. N.K., Thornhill, A. and Lewis, P. (2019) Research Methods for Business Students. 8th ed. Pearson Available at: Available at: https://www.perlego.com/book/971477/research-methods-for-business-students (Accessed: 23 August 2024).

Seeman, J. and Susser, D., (2024) Between privacy and utility: On differential privacy in theory and practice. *ACM Journal of Responsible Computing*, 1(1), Article 3. Available at: https://doi.org/10.1145/3626494 [Accessed 10 July 2024].

Schrems II, (2020) Case C-311/18, *Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems*. ECLI:EU:C: 2020:559.

Staunton, C., Adams, R., Anderson, D., Croxton, T., Kamuya, D., Munene, M. and Swanepoel, C., (2020) Protection of Personal Information Act 2013 and data protection for health research in South Africa. *International Data Privacy Law*, 10(2), pp.160-179. Available at: https://doi.org/10.1093/idpl/ipz024 [Accessed 24 July 2024].

Svantesson, D. (2020) 'Data localization trends and challenges: considerations for the review of the privacy guidelines', *OECD Digital Economy Papers*, No. 301, OECD Publishing, Paris. Available at: https://doi.org/10.1787/abc123 (Accessed: 20 June 2024).

United Nations. (1948) *Universal Declaration of Human Rights*. Available at: https://www.ohchr.org/en/human-rights/universal-declaration/translations/english (Accessed: 1 August 2024).

World Economic Forum (2017) The Fourth Industrial Revolution: What It Means, How to Respond. Available at: https://www3.weforum.org/docs/WEF_Center_4th_Industrial_Revolution.pdf (Accessed: 20 June 2024).

Voigt, P. and Bussche, A.V.D., (2021) *The EU General Data Protection Regulation (GDPR): A Practical Guide*. 2nd ed. Cham: Springer International Publishing.

Yeon, T. (2019) 'The separability of law and morality as an intriguing conundrum within legal positivism: Lessons from *The Concept of Law*.'

APPENDICES

Appendix A – Interview Questions (Set 1).

Preliminary Questions:

i) Have you received, reviewed, and understood the consent form shared with you?
ii) Do you consent to being recorded and quoted for this research?
iii) Do you have any concerns before we begin?

Interview Questions:

1) Can you describe your introduction to law, and how you got involved in data privacy law?
2) The core principles of the GDPR (General Data Protection Regulation) and Data Privacy Act (2018) are accuracy, data minimization, lawfulness, transparency, and purpose limitation. In your line of work, do you think these principles are upheld?
3) How would you best describe 'cross-border' data transfers?
4) Do you believe in the free flow of data? (Why)?
5) There are notable challenges when the concept of data sovereignty is discussed, how can you best describe what this means for legal practitioners and 'for-profit' entities in Ireland?
6) Are you familiar with the Shrems I and II cases? If so, make commentary on how they could positively inform the operation of businesses in Ireland.
7) What is the most common challenge that 'for-profit' entities experience with compliance, in matters of data flows?
8) Do you think the DPC (Data Protection Commission) is able to meet its caseload?
9) Technology advancements regularly outgrow legal provisions, i.e., AI (Artificial Intelligence) and covert surveillance practices which may be involved in data theft or interference with adequacy approved data flows, what would you propose as a mitigative practice for this?
10) What is your commentary on reduced regulatory action?
11) What do you think the future of Data Privacy will look like?

Appendix B – Interview Questions (Set 2).

Preliminary Questions:

i) Have you received, reviewed, and understood the consent form shared with you?
ii) Do you consent to being recorded and quoted for this research?
iii) Do you have any concerns before we begin?

Interview Questions:

1) Can you please describe your training and experience in data privacy in Kenya?
2) Can you provide a succinct overview of the main provisions of the 2019 Data Protection Act?
3) How do you think the Data Provision Act 2019 has provided for cross-border data transfers out of Kenya?
4) What roles does the Office of the Data Protection Commissioner Serve?
5) How effective has the Office of the Data Protection Commissioner been in protecting Kenya's Privacy?
6) In your opinion, are the resources provided for the operation of the ODPC sufficient?
7) What difficulties are experienced in the Kenyan data privacy landscape to facilitate cross-border data transfers?
8) Do global market players meet regulatory requirements? (Do you believe they are effectively penalized for non-compliance?)
9) In what ways is the ODPC taking (or not, in your opinion) regulatory action against non-compliant businesses?
10) Which technology solutions are the most effective to facilitate and ensure data privacy in the Kenyan landscape?
11) In light of controversies surrounding Cambridge Analytica, the Huduma Number controversy, and the alleged election-related scandal linked to the French company Idemia, what steps do you think the ODPC should take to enhance the security of Kenyan citizens?
12) What steps ought to be implemented to improve data security for businesses in Kenya?

APPENDIX – C

(Separate document with transcripts as they are lengthy and explore sensitive topics discussing matters on privacy (and confidentiality), governance and the involvement of the government instruments in citizen's lives.)