THE ROLE AND LIABILITY OF INTERNET SERVICE PROVIDERS IN SOUTH AFRICA: A CRITICAL AND COMPARATIVE APPRAISAL

by

Celeste Zara Nameka

Submitted in accordance with the requirements for the degree

DOCTOR OF LAWS

at

UNIVERSITY OF SOUTH AFRICA

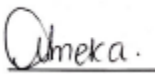
SUPERVISOR: PROFESSOR MG KARELS

2024

DECLARATION

I declare that " *The role and liability of internet service providers in South Africa: A critical and comparative appraisal*" is my original work. All the sources I have relied upon or quoted have been indicated and acknowledged using a complete reference.

Signed at Kimberly this 31st day of August 2024.



Celeste Zara Nameka

Student number: 43735312

ACKNOWLEDGEMENTS

This thesis became a reality with the kind support of many individuals. I want to extend my sincere thanks to all of them.

I want to express my special gratitude and thanks to my supervisor, Dr MG Karels, for her guidance and supervision.

A special tribute goes to my son, Zenande Nameka and my brother in heaven, Nathan Ferris.

ABSTRACT

This research uses a comparative approach to explore the role and liability of internet service providers in South Africa. The research aims to analyse and compare the role and liability of internet service providers for crimes and civil infractions committed by content providers and/or internet users. Against this aim, the researcher argues that internet service providers, as intermediaries, are ideally placed to monitor and control illicit content provision and/or internet use by the end user. The research focuses on South Africa, China, Ireland, and Nigeria. The research interrogated legislative control and queried the fitness for purpose of these mechanisms for internet service providers and the lacunae created by a rapidly expanding digital world comparatively. The research points out recurrent controversial and problematic concerns that affect both the internet service provider and the consumer. The researcher further explores challenges in applying legal imperatives to internet service providers that affect their end users.

The comparative analysis assists in indicating how internet service providers operate in practice and their control (or lack thereof) by various legal frameworks. The researcher makes recommendations and offers solutions to assist with the future role and development of internet service providers and their impact on the end-user and criminal justice system.

KEY TERMS

Electronic Communications and Transactions Act 25 of 2002, freedom of expression, internet service provider, internet users, liability, South Africa, right to privacy.

SOTHO ABSTRACT

Patlisiso ena e sebelisa mokhoa o hlokolosi le oa papiso ho hlahloba karolo le boikarabello ba bafani ba litšebeletso tsa inthanete Afrika Boroa. Boithuto bona bo ikemiselitse ho sekaseka le ho bapisa karolo le boikarabello ba bafani ba litšebeletso tsa inthanete bakeng sa litlolo tsa molao (kapa litlolo tse ling tsa sechaba) tse entsoeng ke bafani ba litaba le/kapa basebelisi ba inthanete. Khahlanong le sepheo sena, mofuputsi o pheha khang ea hore bafani ba litšebeletso tsa marang-rang, e le bakena-lipakeng, ba behiloe ka nepo ho beha leihlo le ho laola phano ea litaba tse seng molaong le/kapa tšebeliso ea inthanete ke mosebelisi oa ho qetela. Patlisiso e shebane le Afrika Boroa, China, Ireland le Nigeria. Patlisiso e botsitse taolo ea molao mme e botsitse ho tšoaneleha molemong oa mekhoa ena bakeng sa bafani ba lits'ebeletso tsa marang-rang le lacunae e entsoeng ke lefatše la dijithale le ntseng le hola ka potlako. Patlisiso e supa likhang tse etsahalang khafetsa le mathata a amang mofani oa litšebeletso tsa inthanete le moreki. Mofuputsi o tsoela pele ho hlahloba liphephetso mabapi le ho sebelisa litlhokahalo tsa molao ho bafani ba litšebeletso tsa inthanete tse amang basebelisi ba bona ba ho qetela.

Tlhahlobo ea papiso ea libaka tse fapaneng e thusa ho bonts'a hore na bafani ba litšebeletso tsa marang-rang ba sebetsa joang le taolo ea bona (kapa khaello ea eona) ka mekhoa e fapaneng ea molao. Mofuputsi o etsa likhothaletso le ho fana ka litharollo ho thusa ka karolo le nts'etsopele ea nako e tlang ea bafani ba litšebeletso tsa inthanete le phello ea bona tsamaisong ea toka ea mosebelisi le ea botlokotsebe.

LIEKETSENG TLHOKO

Electronic Communications and Transactions Act 25 of 2002, tokoloho ea ho itlhalosa, mofani oa litšebeletso tsa inthanete, basebelisi ba marang-rang, boikarabelo, Afrika Boroa, tokelo ea boinotši.

ZULU ABSTRACT

Lolu cwaningo lusebenzisa indlela ebucayi neqhathaniswayo ukuhlola indima nesibopho sabahlinzeki bezinsizakalo ze-inthanethi eNingizimu Afrika. Ucwaningo luhlose ukuhlaziya ngokujulile futhi kuqhathanise indima nesibopho sezomthetho sabahlinzeki besevisi ye-inthanethi ngobugebengu (noma ezinye iziphambeko zomphakathi) ezenziwa abahlinzeki bokuqukethwe kanye/noma abasebenzisi be-inthanethi. Ngokumelene nale nhloso, umcwaningi uphikisa ngokuthi abahlinzeki besevisi ye-inthanethi, njengabalamuli, babekwe ngokufanelekile ukuqapha nokulawula ukunikezwa kokuqukethwe okungekho emthethweni kanye/noma ukusetshenziswa kwe-inthanethi ngumsebenzisi wokugcina. Ucwaningo lugxile eNingizimu Afrika, eChina, e-Ireland naseNigeria. Ucwaningo lwaphenya ukulawulwa komthetho futhi lwabuza ukufaneleka kwenhloso yalezi zindlela zabahlinzeki besevisi ye-inthanethi kanye ne-lacunae edalwe umhlaba wedijithali okhula ngokushesha. Ucwaningo luveza ukukhathazeka okuphindelelayo okuyimpikiswano kanye nezinkinga ezithinta kokubili umhlinzeki wesevisi ye-inthanethi kanye nomthengi. Umcwaningi uphinde ahlole izinselele ekusebenziseni izimfuneko ezingokomthetho kubahlinzeki besevisi ye-inthanethi abathinta abasebenzisi babo bokugcina.

Ukuhlaziywa okuqhathanisayo kwezindawo ezahlukene kusiza ekuboniseni ukuthi abahlinzeki besevisi ye-inthanethi basebenza kanjani kanye nokulawula kwabo (noma ukuntuleka kwakho) ngezinhlaka zezomthetho ezihlukahlukene. Umcwaningi wenza izincomo futhi unikeza izixazululo zokusiza ngendima yesikhathi esizayo nokuthuthukiswa kwabahlinzeki besevisi ye-inthanethi kanye nomthelela wabo ohlelweni lwezobulungiswa bobugebengu obungabasebenzisi bokugcina.

IMIGOMO EYINGQONDO

I-Electronic Communications and Transactions Act 25 ka-2002, inkululeko yokukhuluma, umnikezeli wesevisi ye-inthanethi, abasebenzisi be-inthanethi, isikweletu, iNingizimu Afrika, ilungelo lobumfihlo.

ACRONYMS & ABBREVIATIONS

ACLU	American Civil Liberties Union
ADSL	Asymmetric Digital Subscriber Line
AI	Artificial Intelligence
AOL	America Online
AU	African Union
AXIS	African Internet Exchange System
CAC	Cyberspace Administration of China
China	People's Republic of China
CIS	Chinese Internet System
CJEU	Court of Justice of the European Union
ComReg	Commission for Communications Regulation
CSAI	Cyber Security Artificial Intelligence
CSAM	Child Sexual Abuse Material
DDoS	Distributed Denial-of-Service
DG	Director General
DMCA	Digital Millennium Copyright Act 17 U.S. Code
DRM	Digital Rights Management
DSL	Digital Subscriber Line

EAC	East African Community
ECAA	Electronic Communications Amendment Act 1 of 2014
ECHR	European Court of Human Rights
ECHR	European Court of Human Rights
ECNS	Electronic Communications Networks and Services
E-COMMERCE	Electronic Commerce
ECOWAS	Economic Community of West African States
ECTA	Electronic Communications and Transactions Act 25 of 2002
ECTAB	Electronic Communications and Transactions Amendment Bill of 2012
EFCC	Economic and Financial Crimes Commission (Establishment) Act, 2004.
EU	European Union
GATS	General Agreement on Trade in Services
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation
ICASA	Independent Communications Authority of South Africa
ICCPR	International Covenant on Civil and Political Rights
ICT	Information and Communications Technology

IGF	Internet Governance Forum
IGF	Internet Governance Forum
IMF	International Monetary Fund
IoT	Internet of Things
IPR	Intellectual Property Rights
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
ISS	Information Security Society
IT	Information Technology
ITRs	International Telecommunication Regulations
ITU	International Telecommunication Union
IXP	Internet Exchange Port
JIT	Just In-Time
MFA	Multi-factor authentication
MIIT	Ministry of Industry and Information Technology
NCC	Nigerian Communications Commission
NDPR	Nigerian Data Protection Regulation
NIS	Network and Information Systems Security

NITDA	National Information Technology Development Agency Act, 2007.
NITEL	Nigerian Telecommunications Limited
NSF	National Science Foundation
NSFNET	National Science Foundation Network
P2P	Peer to Peer
PAIA	Promotion of Access to Information Act 2 of 2000
PAIA	Promotion of Access to Information Act
PGMC	Interim Provisions Governing Management of Computer Information Networks
PIPL	Personal Information Protection Law
POPIA	Protection of Personal Information Act
R&D	Research and Development
RICA	Regulation of Interception of Communications and Provision of Communication-Related Information Act of 2002
SA	South Africa
SABAM	Société d'Auteurs Belge – Belgische Auteurs
SABRIC	Banking Risk Information Centre of South Africa
SCC	Senate Committee on Cybercrime

SDG	Sustainable Development Goals
SSA	State Security Agency
UK	United Kingdom
UN	United Nations
USA	United States of America
VoIP	Voice Over Internet Protocol
VPN	Virtual Private Networks
Wi-Fi	Wireless Fidelity
WSIS	World Summit on the Information Society
WTO	World Trade Organisation
ZAR	South African Rand

TABLE OF CONTENTS

CHAPTER ONE

CONCEPTUALISATION AND METHODOLOGY

1.1 INTRODUCTION

This research aims to analyse and compare the role and liability of internet service providers[1] for crimes (or other civil infractions) committed by content providers and/or internet users. Against this aim, the researcher argues that ISPs, as intermediaries, are ideally placed to monitor and control illicit content provision and/or internet use by the end user. In pursuance of the former and latter, in this chapter, the researcher contextualises the research and discusses the background upon which the study is grounded. The content introduces the identified problem statement, methodology, central research concepts, research aim, objectives and values, and the limitations encountered throughout the research process. The overall purpose of the chapter is to contextualise the research question(s) and clarify the methodology used to explore the relevant concept within the context of South African and comparative ISPs, content providers and users.

1.2 RESEARCH BACKGROUND

It is trite that global internet use has shown a significant annual increase.[2] As the worldwide levels of social and economic interconnectedness increase, the widespread adoption of internet technologies remains one of the defining features of such interconnectivity.[3] In line with this, research[4] indicates a noticeable spike in the number of people in emerging economies and developed countries who claim they can access

---

1 Hereinafter referred to as ISP or ISPs, context dependent.

2 Statista https://www.statista.com/statistics/617136/digital-population-worldwide/ (Date of use: 22 January 2024).

3 Gray Group International https://www.graygroupintl.com/blog/globalization (Date of use: 13 January 2023).

4 Elucidated later in this chapter.

the internet.[5] Statistical trends indicate an increase from 3,185,996,155 billion to 3,424,971,237 billion home internet users from 2015 to 2016,[6] which shows a 3.3 per cent global increase in internet use.[7]

As of 2023, approximately 67 per cent of the world's population, or 5.4 billion people, are using the internet, representing an increase of 45 per cent since 2018, with 1.7 billion people going online during that period.[8] Notably, Northern Europe boasts the highest internet penetration rate at 98 per cent, followed by Western Europe at 94 per cent and Northern America at 93 per cent. However, the penetration rates in Southern Asia and Western Africa are lower, at 46 and 43 per cent, respectively.[9] The number of people off-line during 2023 decreased to an estimated 2.6 billion, 33 per cent of the global population. In low-income countries, internet usage is much lower, with only 27 per cent of the population using the internet, compared to 93 per cent in high-income countries.[10] In the United States, 91.56 per cent of adults were reported to use the internet in 2023, a slight increase from 90.81 per cent in 2022.

Additionally, 54.4 per cent of the global internet traffic in 2021 was generated from mobile devices, a significant increase from the 0.7 per cent reported in 2009.[11] The number of fixed broadband subscriptions globally reached 1.4 billion in 2022, showing a steady increase from previous years.[12] Moreover, online time declined by almost 5 per cent year-on-year as of 2023, with the typical user reducing their internet usage by 20 minutes

---

5 Nasdaq https://www.nasdaq.com/articles/internet-usage-within-developing-markets-has-soared (Date of use: 14 August 2023).

6 “Internet users worldwide” http://www.internetlivestats.com/internet-users (Date of use: 21 January 2016).

7 “Internet users worldwide” http://www.internetlivestats.com/internet-users (Date of use: 21 January 2016).

8 International Telecommunication Union (ITU), "Facts and Figures 2023 - Internet Use," https://www.itu.int (Date of use: 21 January 2023).

9 "Internet User Statistics in 2024 — (Global Demographics)," www.demandsage.com (Date of use: 9 January 2024.

10 International Telecommunication Union (ITU), "Facts and Figures 2023 - Internet Use," https://www.itu.int (Date of use: 21 January 2023).

11 "Internet User Statistics in 2024 — (Global Demographics)," www.demandsage.com (Date of use: 9 January 2024).

12 "Internet User Statistics in 2024 — (Global Demographics)," www.demandsage.com (Date of use: 9 January 2024).

per day compared to the previous year.[13] These statistics provide a comprehensive overview of global internet usage, highlighting the ongoing growth in internet access worldwide and the persistent digital divide between different regions and income levels.[14]

Further, internet access and use are widespread in developed countries, but the trends in developing countries suggest that emerging economies are still playing catch-up.[15] In 2013, a study on twenty-one emerging economies indicated a median of 45 per cent in terms of their internet accessibility. The same survey revealed that the median arose primarily because of increased smartphone access.[16]

In 2015, another internet access study in the same emerging economies reported that their median had increased to 54 per cent. The survey tied the 10 per cent surge to increased internet access in countries like The People's Republic of China,[17] Brazil, and Malaysia. In contrast, a 2015 survey on internet access in eleven developed nations revealed a median of 87 per cent.[18] The study showed that more than 87 per cent of consumers in advanced economies like South Korea, Japan, Australia, Israel, Germany, France, Canada, the UK, and the United States of America[19] could access high-speed internet in their households.[20]

Studies suggest that advanced and emerging economies had a 33 per cent gap in internet access.[21] The outcome lends credence to the view that global internet use is increasing rapidly but that such use is concentrated in advanced economies and a small percentage in emerging economies like Brazil, China, and Malaysia. Despite the difference in the rate of advancement and entrenchment of internet use, internet access and use are rapidly growing and look to become a globally entrenched resource shortly,

---

13 DataReportal, "Digital 2023: Global Overview Report," https://www.datareportal.com (Date of use: accessed 9 January 2023).
14 Lembani et al. 2020: 73.
15 Poushte 2016: 3.
16 Poushte 2016: 3.
17 Hereinafter referred to as China.
18 Poushte 2016: 3.
19 Hereinafter referred to as USA.
20 Poushte 2016: 3.
21 Poushte 2016: 3.

whether via traditional computer access or smartphone use. The mechanism of access may differ, but the use remains constantly increasing.

The dominance of advanced economies on internet accessibility extends to smartphone ownership. The rate of smartphone ownership in developed countries is higher than the rate of smartphone ownership in emerging economies. The PEW Research Center's statistics suggest a significant smartphone ownership gap exists between developed and developing countries. [22]

According to the statistics, the gulf in smartphone ownership was 31 per cent.[23] However, the divide between the advanced and emerging economies regarding smartphone ownership is narrowing. Statistics on smartphone ownership suggest that developing countries are recording a significant spike in smartphone ownership rates. According to the statistics, median smartphone ownership spiked to 37 per cent in 2015 from the 21 per cent reported in 2013.[24]

This increase in the rate of smartphone ownership has been a strong contributor to increased internet access in developing countries. Data from developing countries suggest that individuals who report having access to the internet state that they access the internet through their smartphones.

The African continent is home to a sizeable proportion of the global population. Still, the internet access and smartphone ownership trends are markedly different from the observed trends in the rest of the world. The African continent comprises 16 per cent of the world's population, with 9.4 per cent of the global internet user population.[25] Within the statistical context of Africa, South Africa is outmatched by Egypt and Nigeria

---

22 Poushte 2016: 3.
23 Poushte 2016: 3.
24 Poushte 2016: 3.
25 There are 333,521,659 million personal home internet users of the total population of 185,529,578 billion people. See "African internet users" Internet World Stats http://www.internetworldstats.com/stats1.htm (Date of use: 21 January 2016).

regarding internet usage.[26] The latter may be attributed to larger population bases. Although Egypt represents the highest connectivity rate utilizing private internet use, the Egyptian population experiences occasional internet connectivity difficulties. These difficulties may be attributed to governmental interference and shutdowns during times of conflict, such as interruptions during the Arab Spring Revolution in 2011 or power outages caused by too much strain on the electrical sources within the country.[27]

In Nigeria, connectivity problems are related to governmental interference and some extraordinary strains on the power systems.[28] The connectivity difficulties may also arise from low levels of economic development. Low levels of economic development undermine the ability of a government to invest in broadband connectivity or to attract companies that can provide reliable broadband connectivity.[29] Therefore, a weak infrastructure means Africans must grapple with internet connectivity challenges. This is no more apparent than in South Africa, where current load-shedding challenges constantly disrupt access to the internet.

However, the outlined connectivity problems have not dampened the frequency with which Africans and others from developing countries access the internet. Statistics from the PEW Research Center [30] suggest that emerging economies in Africa and other continents are outmatching the advanced economies in social media use, for example.[31]

According to the PEW Research Center statistics, the most enthusiastic users of social media networks come from regions and continents like Africa, Latin America, and the

---

26 Internet World Stats http://www.internetworldstats.com/stats1.htm (Date of use: 21 January 2016).

27 "Emerging nations embrace internet, mobile technology" *Pew Research Center* http://www.pewglobal.org/2014/02/13/emerging-nations-embrace-internet-technology (Date of use: 21 January 2016).

28 http://www.pewglobal.org/2014/02/13/emerging-nations-embrace-internet-mobile-technology (Date of use: 21 January 2016).

29 Reddick et al., 2020: 189.

30 Poushte 2016: 3.

31 http://www.pewglobal.org/2014/02/13/emerging-nations-embrace-internet-mobile-technology (Date of use: 21 January 2016).

Middle East.[32] These statistics suggest that the median rate of the use of social networking sites is 76 per cent in Africa, 82 per cent in Latin America, and 86 per cent in the Middle East.[33]

By comparison, the median rate of social media use is 65 per cent for Europe, 66 per cent for the Asia Pacific region, and 71 per cent for the USA.[34] These statistics confirm that internet users in less developed and emerging African countries are likelier to use social media technologies than those in advanced economies such as Israel, France, Britain, Canada, and the USA.

While statistics suggest that the Internet is becoming an integral component of people's lives in Africa, it is also clear that Africa relies heavily on outdated and weak technological infrastructure. It is opined that ISPs and content providers in Africa have done little to match the high demand for quality internet and high-quality content in Africa, as is the case for most developed countries.[35] This plays to the role of ISPs in the continent and lends credence to the research interest here, namely the liability of such ISPs to the content provider and end-user.

Many online users in Africa thus rely on content from Europe, the USA, and other developed countries due to the service gaps in the African continent. This leads to a situation where there is a proffered inefficiency of the legal infrastructure for protecting consumers (and indeed the State and government). This discussion also forms part of the research and is included in chapter two.

The internet's widespread use has led to several criminal and civil problems, necessitating a critical appraisal of the role and liability of ISPs.[36] For instance, internet

---

32 http://www.pewglobal.org/2014/02/13/emerging-nations-embrace-internet-mobile-technology (Date of use: 21 January 2016).
33 Poushte 2016: 5.
34 Poushte 2016: 5.
35 "Internet User Statistics in 2024 — (Global Demographics)," www.demandsage.com (Date of use: 9 January 2024).
36 Major 2021: 8.

shutdowns[37] have been used by jurisdictions as a response to various situations, ranging from religious anniversaries and protests to communal violence and exams. In 2023, India imposed 33 shutdowns in different states, affecting millions.[38] Similarly, in Myanmar, internet shutdowns were imposed across all 330 townships at least once in 2022, significantly impacting disaster response during Cyclone Mocha.[39] This trend is not limited to one region; for example, Turkish authorities throttled access to Twitter following an earthquake in February, hampering humanitarian efforts.[40]

Moreover, the evolution of technology has significantly increased the potential and complexity of cybercrime.[41] The next decade is expected to see an increase in the speed and coverage of connectivity, which will contribute to a rise in the volume and speed at which different types of cybercrime are conducted.[42] The proliferation of IT-enabled devices, systems, and services will increase the attack surface and vulnerabilities that malicious actors could leverage.[43] Additionally, the growing sophistication of cybercrime, as indicated by the increased use of ransomware and the targeting of supply chains, has raised concerns for both the public and private sectors.[44]

These developments suggest that ISPs, as intermediaries, have a significant role in monitoring and controlling illicit content and internet use. The liability of ISPs in this context becomes a pertinent issue, as they are uniquely positioned to oversee and

---

37 Access Now, "Internet Shutdowns in 2023: A Mid-Year #KeepItOn Update," https://www.accessnow.org (Date of use: 9 January 2024).

38 Access Now, "Internet Shutdowns in 2023: A Mid-Year #KeepItOn Update," https://www.accessnow.org (Date of use: 9 January 2024).

39 Access Now, "Internet Shutdowns in 2023: A Mid-Year #KeepItOn Update," https://www.accessnow.org (Date of use: 9 January 2024).

40 Access Now, "Internet Shutdowns in 2023: A Mid-Year #KeepItOn Update," https://www.accessnow.org (Date of use: 9 January 2024).

41 Sorbán 2019: 19.

42 Rand, "The Future of Cybercrime in Light of Technology Developments," https://www.rand.org (Date of use: 9 January 2024).

43 Rand, "The Future of Cybercrime in Light of Technology Developments," https://www.rand.org (Date of use: 9 January 2024).

44 The National, "Top 12 Cyber Crime Trends to Watch for in 2023," https://www.thenationalnews.com (Date of use: 9 January 2024). Weiss 2023, "The Year Ahead: Key Cybersecurity and Privacy Issues for 2023," https://www.paulweiss.com (Date of use: 9 January 2024).

potentially mitigate some of these risks. Given the critical role of ISPs in the modern digital infrastructure, understanding and defining their responsibilities and liabilities while considering these emerging threats is crucial.

Like the internet and content providers, the response of governments and other policymakers in the African continent has been slow. Despite the high rates of internet use and the unprecedented use of social media technologies, governments in African countries like Nigeria, South Africa, and Egypt are yet to enact a fully-fledged and practical framework of cyber laws that can govern the interaction between internet users, content providers, and ISPs. It is opined that many existing laws do not provide the safeguards needed to protect the government, consumers, and other stakeholders from the adverse consequences that might arise from the interaction between internet users, content providers, and ISPs. This is especially worrying considering that an unregulated ICT environment can significantly threaten consumers, the government, and African society.

Although research suggests that South African consumers fail to take personal responsibility for the security of their personal information online,[45] resulting in a high incidence of cybercrime, the reality is that the absence of adequate legal infrastructure is the leading cause of the high incidence of cybercrime. An analysis of the existing cyber laws suggests that they do not go far enough to protect consumers from cybercrimes. The existing laws merely list the types of crimes committed on the internet and the range of sentences that culprits will face in the event of conviction. Still, they do not punish ISPs and content providers for creating the types of vulnerabilities that increase the susceptibility of South African consumers to cyber-attacks. Indeed, an analysis of existing and proposed cyber laws confirms that they have no provisions that give security agencies and the courts the authority to issue punitive penalties to content providers and ISPs for vulnerabilities that render South African consumers susceptible to cybercrime.[46]

45 Mapangavanhu & Kerchhoff 2023: 11.
46 Fernandez Nieto 2022: 11.

However, the introduction of the Cybercrimes Act 19 of 2020 in South Africa marks a significant step in the country's cyber governance and policy approach. This Act creates offences related to cybercrime and prescribes penalties, aiming to curb the increasing trend of cybercrime, improve national security, and hold cybercriminals accountable.[47] Despite these advancements, the Act's interplay with the Protection of Personal Information (POPI) Act could lead to potential conflicts and liability issues when cyber incidents occur.[48]

A further challenge lies in implementing the Cybercrimes Act, given the South African Police Service's limited resources and (in)experience in dealing with cybercrime. The Act mandates the police to establish a 24/7 point of contact for all cybercrime reporting within a year after the legislation's enforcement, emphasizing the need for capacity building and international cooperation.[49] Furthermore, while the Act clearly defines cybercrimes, including unlawful access, data interception, online forgery, fraud, and extortion, it raises concerns about balancing security, privacy, and personal freedom during cybercrime investigations. This balance is crucial, especially considering that organisations might hesitate to report cyber incidents if they reveal their failure to take necessary precautions, potentially exposing them to sanctions under the POPI Act.[50]

1.3 PROBLEM STATEMENT

Technology often develops more rapidly than a country’s legal and institutional abilities to pass and enforce laws regulating technology. South Africa’s governmental challenges are like those of other nations[51] regarding establishing legal boundaries, definitions, and

47 Aon South Africa, "Cybercrimes Act Report 2023," https://www.aon.co.za (Date of use: 9 January 2024).
48 ISS Africa, "South Africa Lays Down the Law on Cybercrime," https://www.issafrica.org (Date of use: 9 January 2024).
49 ISS Africa, "South Africa Lays Down the Law on Cybercrime," https://www.issafrica.org (Date of use: 9 January 2024).
50 ISS Africa, "South Africa Lays Down the Law on Cybercrime," https://www.issafrica.org (Date of use: 9 January 2024).
51 For example, Nigeria, and Egypt.

parameters on telecommunication and internet technology, data laws, and the difficulties in accessing the internet.

This research, therefore, aims to investigate the role and liability of ISPs in South Africa. It relies on a comparative methodology (discussed later in this chapter) to analyse various concepts connected to ISPs (such as the interaction between ISPs, content providers and end-users) and the legislation applicable to their function and liability in comparison jurisdictions.

The focus of the research is thus:

i. The role of the ISP, which provides services for accessing and using the Internet); and
ii. The legal liability of the ISP in terms of statutory and secondary liability.

The following research components are central to the research: ISPs, content providers, internet users, security and cryptography, copyright and file sharing, regulatory compliance, spam, licensing, Cyber Security Artificial Intelligence (CSAI), Child Sexual Abuse Material (CSAM) / Minors, Online gambling, limitation of liability for ISP activities, industry bodies, advertising, inception and monitoring; and customer registration.

Below, the researcher conceptualises working definitions for the above central themes relevant to this research.

1.4 CONCEPTUAL DEFINITIONS

1.4.1 INTERNET SERVICE PROVIDER

ISPs are the backbone of the digital age, serving as the essential link that connects individuals and businesses to the vast world of the internet. These companies or organisations offer internet access services, allowing users to tap into the immense pool

of information, communication, and resources available on the World Wide Web.[52] The role of ISPs is pivotal in shaping how we interact with and depend on the digital realm.

At its core, an ISP acts as the gateway to the internet for its subscribers. Whether a student conducting research, a business conducting e-commerce, or an individual seeking entertainment, ISPs provide the infrastructure and connectivity necessary to access the online world. They maintain a complex network of hardware and software components that facilitate data transmission between users and the multitude of servers, websites, and online services that make up the Internet.[53]

One of the defining features of ISPs is the diverse range of internet services they offer. Users can choose from various options to suit their specific needs, such as broadband, DSL (Digital Subscriber Line), fibre-optic, or wireless connections. Broadband services have become particularly popular, offering high-speed internet access that has transformed how we consume digital content, communicate, and conduct business online.[54] DSL, which uses telephone lines, is an improved alternative to traditional dial-up connections, providing a faster and more stable experience. Fibre-optic connections, known for their lightning-fast speeds and low latency, rely on data transmission using light signals, setting the benchmark for high-speed internet. Additionally, wireless ISPs use technologies like Wi-Fi and cellular networks, enabling users to connect their devices without the constraints of physical cables.[55]

ISPs are the unsung heroes of the digital age, seamlessly enabling our connected lifestyles. They serve as the intermediaries that ensure data packets reach their intended destinations across the global internet infrastructure.[56] Without ISPs, the intricate web of communication, information sharing, and online services that define our daily lives would be impossible.

---

52 Gillis 2022: 3.
53 Verizon 2022:4.
54 Gillis 2022: 3.
55 Sheehy 2017: 1.
56 Gillis 2022:4.

However, ISPs face various challenges and responsibilities as internet gatekeepers. They handle vast amounts of user data, making data privacy and security paramount concerns. To protect against cyber threats and safeguard user information, ISPs must implement robust cybersecurity measures. Additionally, net neutrality remains a hotly debated issue in many countries, as it advocates for ISPs to treat all internet traffic equally without discriminating or prioritizing specific content or services.[57]

Regulatory compliance is another significant responsibility for ISPs, as they must adhere to local, national, and international regulations governing their operations. Compliance with laws related to data retention, user privacy, and content filtering is essential to avoid legal issues and maintain public trust. Furthermore, ISPs are increasingly focused on addressing the digital divide, making internet access accessible to underserved and remote areas, thus ensuring that no one is left behind in the digital age.

1.4.2 CONTENT PROVIDER

In the digital era, content providers play a pivotal role in shaping our online experiences by serving as the creators and suppliers of digital content. These entities, from individual bloggers and YouTubers to massive media conglomerates and e-commerce giants, produce and disseminate diverse digital materials that enrich the online landscape.[58] The content they generate spans various forms, encompassing text, images, videos, audio, software, and much more.

The content provider delivers internet users valuable and engaging information, entertainment, and services. Individual content creators, such as bloggers and vloggers, often use their platforms to share personal experiences, expertise, or artistic creations with a global audience.[59] They connect with their followers personally, offering unique perspectives, insights, and entertainment catering to niche interests.

---

57 Eloff 2020: 19.
58 Duffett et al. 2019: 604.
59 Duffett et al. 2019: 609.

On a larger scale, media companies and streaming platforms produce a wide range of content, including news articles, television shows, movies, music, and podcasts, to satisfy the diverse tastes of internet users. These entities often invest substantial resources in content creation, employing professionals in various fields such as journalism, filmmaking, and music production to deliver high-quality experiences.[60]

E-commerce websites also fall under the category of content providers, as they curate product listings, images, and descriptions to entice consumers to make purchases.[61] The content on these platforms is designed to inform and persuade, creating a seamless shopping experience for online customers. The collective efforts of content providers contribute significantly to the richness and diversity of online content. They give rise to a virtual ecosystem where users can access information, learn new skills, enjoy entertainment, and connect with like-minded individuals. Content providers drive user engagement, attract audiences, and generate revenue through advertising, subscriptions, or product sales.[62]

However, the role of content providers also comes with responsibilities and challenges. They must exercise ethical standards in content creation and dissemination as they wield the power to influence and shape public opinion. Issues related to fake news, misinformation, and spreading harmful content underscore the importance of responsible content production.[63] Furthermore, content providers must navigate copyright and legal matters to ensure they have the appropriate rights to use and distribute their shared materials. They also face challenges in online privacy, data security, and adapting to evolving technologies and user preferences.

60 Duffett et al. 2019: 604.
61 Gillis 2022:10.
62 Duffett et al. 2019: 604.
63 Duffett et al. 2019: 604.

1.4.3 INTERNET USER

Internet users encompass a vast and diverse global community with unique motivations and purposes for accessing the Internet. These individuals and entities are the lifeblood of the digital age, connecting to the World Wide Web through various devices, from smartphones and tablets to laptops and desktop computers. Internet users are united by their shared quest for information, communication, entertainment, and opportunities for online engagement.

One of the primary functions of internet users is information retrieval.[64] With the wealth of online knowledge, users can access news, research, educational resources, and a wide range of information on any topic. This access to information has democratized learning and research, allowing people from all walks of life to expand their knowledge and horizons.[65]

Communication is another cornerstone of internet usage. Email, instant messaging, social media platforms, and video conferencing tools enable users to connect with friends, family, colleagues, and acquaintances across the globe in real-time. This interconnectedness has transformed how people stay in touch, collaborate, and build communities, transcending geographical boundaries.

Entertainment is a significant driver of internet activity, with users streaming videos, music, and interactive games.[66] Online shopping has also revolutionized the retail landscape, allowing consumers to browse, purchase, and receive products and services conveniently from their devices.[67] Additionally, internet users engage in various online activities such as blogging, creating content, and participating in online forums, contributing to the vibrant digital culture. However, the digital realm comes with its own set of challenges and considerations. Internet users must navigate privacy,

64 Okai-Ugbaje et al. 2020: 49.
65 Mpungose 2020: 6.
66 Duffett et al. 2019: 604.
67 Duffett et al. 2019: 604.

cybersecurity, and responsible online behaviour issues. Being critical consumers of online information and adhering to ethical standards in digital interactions are vital aspects of responsible internet usage.

1.4.4 SECURITY AND CRYPTOGRAPHY

In the digital age, where vast amounts of sensitive information are exchanged over the internet, security and cryptography are indispensable in ensuring online communications and data trustworthiness.[68] Security measures and cryptographic techniques are the guardians of confidentiality, integrity, and authenticity in the digital realm.

Cryptography, the science of encoding and decoding information, is at the heart of modern digital security. It involves using complex mathematical algorithms to transform plain text into ciphertext, rendering it unintelligible to anyone without the appropriate decryption key. This process protects sensitive data, such as financial transactions, personal information, and government communications.[69]

One of the cornerstones of cryptography is encryption, which is converting data into an unreadable format that can only be deciphered by those with the proper cryptographic keys.[70] This ensures that even if unauthorized individuals gain access to encrypted data, they cannot make sense of it. Public-key encryption, for instance, employs both a public key for encryption and a private key for decryption, adding an extra layer of security.

Beyond cryptography, broader security measures encompass various strategies and technologies to safeguard digital assets. These measures include firewalls, intrusion detection systems, antivirus software, and multi-factor authentication. Collectively, they

---

68 Fortinet “What is cryptography” https://www.fortinet.com/resources/cyberglossary/what-is-cryptography (Date of use: 9 January 2024).

69 Fortinet “What is cryptography” https://www.fortinet.com/resources/cyberglossary/what-is-cryptography (Date of use: 9 January 2024).

70 Fortinet “What is cryptography” https://www.fortinet.com/resources/cyberglossary/what-is-cryptography (Date of use: 9 January 2024).

work to thwart cyberattacks, such as malware infections, phishing attempts, and denial-of-service attacks.[71]

The significance of security and cryptography extends to every sector of the digital landscape. Financial institutions rely on cryptographic protocols to secure online banking transactions, while e-commerce platforms use them to protect customer payment information. Governments employ strong encryption to safeguard classified information and maintain national security.

As technology evolves, so do the challenges in the realm of security and cryptography. Cybercriminals continually seek innovative ways to breach defences, making it imperative for security experts and cryptographers to stay ahead of threats. Advancements in quantum computing, for instance, pose potential challenges to existing cryptographic methods, leading to ongoing research into quantum-resistant encryption techniques.

1.4.5 COPYRIGHT AND FILESHARING

Copyright and file sharing represent two fundamental aspects of the digital era, each with its unique implications and challenges. Copyright, a legal framework designed to protect creators' intellectual property, intersects with file sharing, a practice transforming how digital content is disseminated and consumed.[72] Copyright grants creators exclusive rights to their original works, including the rights to reproduce, distribute, perform, and adapt their creations.[73] This protection encourages creativity by ensuring creators can benefit from their work and maintain control over its use. It encompasses various creative outputs, from literature and music to software and visual arts.

---

71 Fortinet “What is cryptography” https://www.fortinet.com/resources/cyberglossary/what-is-cryptography (Date of use: 9 January 2024).

72 Aon South Africa, "Cybercrimes Act Report 2023," https://www.aon.co.za (Date of use: 9 January 2024).

73 Aon South Africa, "Cybercrimes Act Report 2023," https://www.aon.co.za (Date of use: 9 January 2024).

On the other hand, file sharing refers to distributing digital files, often over the internet, to multiple recipients.[74] While file sharing can serve legitimate purposes, such as sharing family photos or collaborating on projects, it has also been associated with copyright infringement when individuals share copyrighted materials without proper authorization.[75] This practice, commonly related to peer-to-peer (P2P) file-sharing networks, has raised significant concerns in the digital age. Unauthorized file sharing of copyrighted materials can result in a loss of revenue for creators and content distributors. Music, movies, software, and written works are particularly susceptible to this form of piracy.[76] Copyright holders have employed various strategies, such as Digital Rights Management (DRM) and legal actions, to protect their intellectual property rights.

Efforts to strike a balance between copyright protection and the sharing of information have led to debates and legal battles. Fair use exceptions, for instance, allow limited use of copyrighted material without permission, often for purposes such as criticism, commentary, education, or parody.[77] However, determining what constitutes fair use can be complex and subjective. The digital landscape continues to evolve, necessitating ongoing discussions about copyright law and its adaptation to the Internet age. Violating copyright in a globally connected world is challenging, requiring collaboration among governments, technology companies, and content creators. Finding effective ways to protect intellectual property while promoting the responsible sharing of knowledge and creativity remains crucial in the ever-expanding digital ecosystem.[78]

1.4.6 REGULATORY COMPLIANCE

Regulatory compliance in the context of the Internet is a critical aspect that ensures the responsible and lawful operation of various Internet stakeholders. It encompasses

---

74 Aon South Africa, "Cybercrimes Act Report 2023," https://www.aon.co.za (Date of use: 9 January 2024).
75 Fernando 2022: 22.
76 Aon South Africa, "Cybercrimes Act Report 2023," https://www.aon.co.za (Date of use: 9 January 2024).
77 Okai-Ugbaje et al. 2020: 49.
78 Aon South Africa, "Cybercrimes Act Report 2023," https://www.aon.co.za (Date of use: 9 January 2024).

adherence to a complex web of laws, regulations, and industry standards that govern internet-related activities. These regulations are designed to address a wide range of concerns, from data privacy and cybersecurity to consumer protection and intellectual property rights. ISPs and content providers, among others, bear significant responsibilities in complying with these regulations. ISPs, for instance, must adhere to data privacy laws that govern the collection, storage, and protection of user information.[79] They are also subject to net neutrality rules prohibiting discrimination against or prioritising specific internet traffic.

Content providers, on the other hand, must respect copyright laws, ensuring that they have the appropriate licenses and permissions to use and distribute copyrighted materials. They must also comply with regulations related to online advertising, ensuring transparency and ethical practices in their marketing efforts. Failure to comply with regulatory requirements can result in legal consequences, fines, and damage to reputation. As technology and internet usage evolve, regulatory compliance remains an ongoing challenge, requiring constant adaptation to new legal frameworks and industry standards. Internet stakeholders must remain vigilant in aligning their operations with the ever-changing landscape of Internet regulations to ensure a safe, secure, and lawful online environment for users and businesses.

1.4.7 SPAM

Spam represents a pervasive and persistent issue in the digital world, posing threats to the quality and security of online communication and services. These unsolicited and often unwanted messages flood email inboxes, comment sections, and social media platforms, targeting a broad audience with various malicious intentions. One primary aim of spam is advertising. It inundates users with commercial messages promoting products, services, or scams, often aggressively or deceitfully.[80] Spam emails can promote counterfeit goods, fraudulent investment schemes, or unscrupulous

[79] Major 2021:18. Fernandez Nieto: 2022: 11.
[80] Major 2021:18.

pharmaceuticals, attempting to deceive recipients into making purchases or revealing personal information.[81]

Another sinister aspect of spam involves the dissemination of malware and phishing attacks. Cybercriminals use spam as a delivery mechanism for malicious software, including viruses, ransomware, and spyware.[82] Phishing emails, a subset of spam, impersonate legitimate entities to trick users into disclosing sensitive information like login credentials or financial details.[83] The fight against spam involves various countermeasures, including email filters, blacklists, and user education. Email providers employ advanced algorithms to identify and divert spam messages into separate folders or block them entirely. However, the ever-evolving tactics employed by spammers require continuous adaptation and vigilance.

1.4.8 LICENSING

Licensing is a critical component of the digital age, serving as the legal framework that governs the distribution and use of intellectual property, such as software, music, images, and more.[84] It represents the mechanism through which creators and rights holders grant permission to others to utilize their creations while retaining control over their use. Licensing agreements are legally binding contracts that specify the terms and conditions under which intellectual property can be accessed, used, and shared. [85] These agreements often address various aspects, including the scope of usage, duration, geographical limitations, and financial arrangements, such as royalties or licensing fees.[86] Licensing agreements provide clarity and legal protection for both the

81 Major 2021:18.
82 Fernandez Nieto: 2022: 12.
83 Fernandez Nieto: 2022: 11.
84 Fernandez Nieto: 2022: 17.
85 Aon South Africa, "Cybercrimes Act Report 2023," https://www.aon.co.za (Date of use: 9 January 2024).
86 Aon South Africa, "Cybercrimes Act Report 2023," https://www.aon.co.za (Date of use: 9 January 2024).

rights holder and the licensee, outlining the boundaries within which the intellectual property can be leveraged.

In the context of the internet, licensing plays a crucial role in content distribution and digital services.[87] Music streaming platforms, for example, obtain licenses from record labels and artists to stream copyrighted songs to subscribers. Software companies grant users licenses to install and use their applications.[88] Even open-source software projects use licensing to specify how their code can be modified and distributed.[89] Licensing also intersects with copyright enforcement and DRM. It helps protect intellectual property by defining authorized uses and preventing unauthorized distribution or reproduction. While licensing facilitates the legitimate sharing and monetization of digital content and services, it raises questions about fair use, copyright infringement, and the balance between protecting creators' rights and promoting innovation and creativity.

1.4.9 CSAM/INAPPROPRIATE CONTENT/MINORS

Child Sexual Abuse Material (CSAM), inappropriate content, and the protection of minors on the internet address a critical aspect of online safety and child protection in the digital age.[90] It primarily focuses on the legal, technical, and ethical measures to combat the dissemination of harmful content and safeguard young internet users. Child protection on the internet is of utmost importance, given the prevalence of online threats and the potential exposure of minors to age-inappropriate or explicit material. Governments and regulatory bodies have implemented legal frameworks to criminalize the creation, distribution, and possession of CSAM.[91] These laws are reinforced by strict enforcement measures to bring perpetrators to justice.

---

87 Aon South Africa, "Cybercrimes Act Report 2023," https://www.aon.co.za (Date of use: 9 January 2024).
88 Fernandez Nieto: 2022: 12.
89 Aon South Africa, "Cybercrimes Act Report 2023," https://www.aon.co.za (Date of use: 9 January 2024).
90 Aon South Africa, "Cybercrimes Act Report 2023," https://www.aon.co.za (Date of use: 9 January 2024).
91 Major 2021:23. Fernandez Nieto: 2022: 17.

To protect minors from inappropriate content, various technical solutions have been developed. These include content filtering and parental control tools that allow parents and guardians to restrict access to age-inappropriate websites and materials.[92] Social media platforms and online services often have reporting mechanisms and policies to remove or limit access to content that violates their guidelines.[93]

Education and awareness campaigns are essential components of protecting minors online. These initiatives aim to educate children and adults about safe internet practices, responsible online behaviour, and the potential risks associated with online interactions. They empower young users to make informed decisions and seek help when needed. The multifaceted approach to addressing CSAM, inappropriate content, and child protection on the internet underscores the collective responsibility of governments, technology companies, parents, educators, and internet users. It represents an ongoing effort to create a safe digital environment where minors can explore, learn, and communicate online without exposure to harm or exploitation.[94]

1.4.10 ONLINE GAMBLING

Online gambling refers to betting or wagering on games of chance or skill using internet-based platforms.[95] This digital evolution of traditional gambling activities encompasses various options, including online casinos, sports betting, poker rooms, and more. While it offers convenience and accessibility, online gambling also presents a range of social, legal, and ethical considerations. One critical aspect of online gambling is regulatory oversight. Various jurisdictions have established legal frameworks to govern and license online gambling operators, ensuring fair play, consumer protection, and responsible

92 Major 2021:23. Fernandez Nieto: 2022: 17.
93 Duffett et al. 2019: 611.
94 Okai-Ugbaje et al. 2020: 49.
95 Duffett et al. 2019: 609.

gaming practices.[96] These regulations aim to prevent fraud, money laundering, and addiction while maintaining the industry's integrity.

Responsible gaming practices are another focal point. Online gambling platforms often promote responsible gambling through measures such as setting betting limits, offering self-exclusion options, and providing information on problem gambling resources.[97] These initiatives aim to mitigate the potential harms associated with excessive gambling. However, online gambling can also raise concerns related to addiction, underage gambling, and financial problems. It is imperative for individuals to exercise self-control and for governments and operators to enforce regulations that protect vulnerable populations. Balancing the benefits and risks of online gambling is an ongoing challenge in the digital age, requiring a multifaceted approach to ensure a safe and responsible gaming environment.

1.4.11 LIMITATION OF LIABILITY FOR ISP ACTIVITIES

Limiting liability for ISP activities is a crucial legal provision that addresses the complex intersection of internet usage and copyright enforcement. These provisions aim to strike a delicate balance between protecting the interests of copyright holders and ensuring that ISPs can provide internet access without undue legal burden for the actions of their users.[98] Generally, these provisions shield ISPs from being held directly liable for copyright infringement or other illegal activities their subscribers conduct. Instead, they are viewed as intermediaries merely providing access to the internet. This framework is essential for promoting the growth and accessibility of the Internet as it allows ISPs to function without the constant threat of legal action based on the actions of their users.[99]

However, these legal protections do not grant ISPs absolute immunity. They often require ISPs to respond promptly to copyright infringement notices and implement

96 Aon South Africa, "Cybercrimes Act Report 2023," https://www.aon.co.za (Date of use: 9 January 2024).
97 Duffett et al. 2019: 609.
98 Junda 2021: 44.
99 Fernando 2022: 18.

measures, such as terminating the accounts of repeat offenders, to address illegal activities conducted by their users. The limitation of liability provisions represents a delicate compromise between fostering a free and open internet and protecting intellectual property rights.[100] These provisions have played a pivotal role in shaping the legal landscape of the Internet, acknowledging the unique challenges and responsibilities of ISPs in the digital age.

1.4.12 INDUSTRY BODIES

Industry bodies are essential organisations within the Internet industry that serve as unifying forces, bringing together stakeholders from specific sectors to advance common interests and goals.[101] These bodies play a pivotal role in shaping the digital landscape by establishing standards, promoting best practices, and advocating for the interests of their members. One primary function of industry bodies is developing and maintaining industry standards.[102] These standards ensure interoperability, quality, and consistency in products and services within a particular sector, benefiting consumers and businesses. By setting and maintaining these standards, industry bodies contribute to the stability and growth of their respective industries.

Additionally, these organisations often serve as a collective voice for their members, representing their concerns and interests to governments, regulatory bodies, and the public.[103] They engage in advocacy efforts to influence policies and regulations that impact their industries, helping to create a favourable business environment. Moreover, industry bodies provide a platform for collaboration and networking among their members, fostering knowledge sharing, innovation, and the exchange of ideas. They

100 Fernando 2022: 18.
101 Junda 2021: 47.
102 Fernando 2022: 22.
103 Fernando 2022: 22.

organize conferences, seminars, and working groups to facilitate these interactions, driving progress and growth within their sectors.[104]

1.4.13 ADVERTISING

Online advertising is a cornerstone of the digital economy, enabling businesses to reach their target audiences in the virtual realm.[105] This section delves into the multifaceted world of online advertising, covering various practices, regulations, and emerging challenges. Online advertising encompasses multiple formats, from display adverts and video commercials to native content and social media promotions. It leverages sophisticated algorithms and data analytics to deliver tailored messages to users based on their demographics, interests, and online behaviour.[106]

However, online advertising also raises important user privacy and data protection considerations. As advertisers collect and utilize vast amounts of user data for targeting, transparency and consent become paramount.[107] In some parts of the globe, regulatory frameworks, such as the General Data Protection Regulation (GDPR), have been introduced to safeguard user privacy and require advertisers to obtain explicit consent for data collection and processing.[108] Advert fraud is another significant concern within online advertising. Fraudulent activities, such as click fraud and impression fraud, siphon off advertising budgets and undermine the credibility of digital marketing efforts. Combating advert fraud requires ongoing efforts, including fraud detection technologies and industry collaboration. Balancing the benefits of targeted advertising with user privacy and fraud prevention remains a constant challenge for advertisers, regulatory bodies, and technology companies. Navigating these complexities is essential to ensure

---

104 Aon South Africa, "Cybercrimes Act Report 2023," https://www.aon.co.za (Date of use: 9 January 2024).
105 Aon South Africa, "Cybercrimes Act Report 2023," https://www.aon.co.za (Date of use: 9 January 2024).
106 Fernando 2022: 27.
107 Dharmawan et al. 2019: 3175.
108 Aon South Africa, "Cybercrimes Act Report 2023," https://www.aon.co.za (Date of use: 9 January 2024).

that online advertising continues to drive the digital economy while respecting user rights and maintaining trust in the digital ecosystem.

1.4.14 INCEPTION AND MONITORING

Inception and monitoring are integral for governing internet services and activities, from creation to ongoing oversight. Inception pertains to the initial stages of conceiving and developing internet platforms, technologies, or initiatives.[109] This involves planning, designing, and implementing digital ventures, be it a new website, an online application, or a technology startup.[110] The inception phase is crucial for laying the foundation and setting the strategic direction of these digital endeavours.

On the other hand, monitoring is the continuous and vigilant observation of internet services and activities once they are operational.[111] This process serves multiple purposes, including ensuring compliance with legal and regulatory requirements, maintaining the security and stability of online platforms, and optimizing their performance. Monitoring also involves tracking user behaviour and engagement to gather insights for improvement and adaptation.

Together, inception and monitoring represent the life cycle of internet services and initiatives, encompassing their birth and ongoing care. These processes are vital for developing, operating, and evolving digital endeavours in an ever-changing online landscape.

1.4.15 CUSTOMER REGISTRATION

Customer registration is a fundamental procedure in the digital world, where individuals create accounts or sign up for online services. This process serves multiple purposes, including personalizing user experiences, enhancing security, and enabling access to

109 Dharmawan et al. 2019: 3175.
110 Dharmawan et al. 2019: 3175.
111 Fernando 2022: 29.

various features.[112] Data privacy is critical to customer registration, emphasizing the importance of safeguarding user information. Internet platforms must comply with privacy regulations and inform users about the collection and use of their data. Providing transparency and obtaining user consent are vital steps in maintaining trust.

Authentication methods play a significant role in customer registration, ensuring users are who they claim to be. Passwords, multi-factor authentication (MFA), and biometrics are standard tools to verify user identities and enhance security.[113] Legal requirements and responsibilities associated with customer registration vary by jurisdiction, covering aspects like data protection, age restrictions, and user agreements. Companies are accountable for securing user data and adhering to applicable laws to avoid legal repercussions.[114]

1.5 PURPOSE, AIM AND VALUE OF RESEARCH

There is no denying the expansive role of the internet in our daily lives. Whether via traditional means or the use of cellular technology, the value of the Internet cannot be underestimated. Add to this the recent advances of artificial intelligence (AI), digital transformation, and the rapid expansion of work-from-home technologies, and questions arise as to how this technology can be monitored to prevent abuse, criminality, and harm. Departing from this point, the researcher turns her attention to the role and liability of ISPs simply because it is rare for technology companies to transmit their content directly to the targeted end-users. Instead, they rely on a broad category of ISPs to mediate content dissemination.

ISPs are intermediaries that host access, network, and communications service providers. They offer platforms allowing internet users to share, download, edit, and upload data. From this perspective, the role and liability of ISPs (direct, contributory, or

112 Dharmawan et al. 2019: 3177.
113 Fernando 2022: 33.
114 Fernando 2022: 33.

vicarious) must be examined to determine the limits of their role to content providers and end users.

ISPs are easily identified and are in an excellent position to supervise how their subscribers use the internet. In certain circumstances, ISPs are believed to bear the responsibility for the infringements committed through their systems since they are in an advantageous position to supervise their subscribers. It is, therefore, essential to balance the subscriber interests and the limitations of liability for ISPs.

Consequently, this research is purposed on the role and liability of ISPs. Specifically, it investigates whether governments have justification in their attempt to hold ISPs responsible for the actions of consumers and organisations using their services. This is achieved using a comparative research design focused on a desktop literature review of legislation, case law and academic opinion.

The researcher aims to explore the role and liability of ISPs in South Africa by comparing legislative models employed by comparative jurisdictions. The primary purpose is to inform action, gather evidence for theories, and contribute to developing knowledge in the field of study. The value of this research is not only for the benefit of students and academics but for all professionals and non-professionals interested in the field of study.

1.5.1 RESEARCH AIM

The researcher aims to explore the role and liability of ISPs in South Africa by critically comparing legislative models employed by comparative jurisdictions. To do this, the researcher will investigate the legal framework for ISP liability, compare legal frameworks from other jurisdictions, judge the effectiveness of legislation, and analyse its impact on stakeholders within the broader context of technological advancement and ethical considerations.

1.5.2 RESEARCH PURPOSE

This research aims to persuade readers to understand the role and liability of ISPs in South Africa. The specific purposes of this study are:

- **Examine the Legal Framework and Liability of ISPs**: To systematically analyze and compare the legal frameworks governing ISPs in South Africa with those in selected comparative jurisdictions (China, Ireland, and Nigeria), focusing on the statutory obligations, roles, and liabilities of ISPs concerning cybercrimes and online content regulation.
- **Identify Policy and Legal Recommendations**: To develop informed recommendations and strategies for enhancing the legal and regulatory environment in South Africa, aimed at improving ISP accountability, safeguarding user rights, and addressing contemporary challenges in digital communication and cybersecurity.

1.5.3 RESEARCH VALUE

The academic value of this study is to add to the existing body of knowledge on ISPs in South Africa and contribute to intellectual and practical discourse. The research intends to add to the existing body of knowledge by clarifying and defining the role and liability of ISPs, making recommendations, and providing solutions to the identified phenomenon. The knowledge generated through this study will benefit ISPs, content providers, end-users, the legislature, and arbiters of fact, all of whom are at the forefront of the industrial revolution and digital transformation in South Africa.

1.6 RESEARCH QUESTION(S)

This study aims to dissect the multifaceted role and legal responsibilities of ISPs in South Africa, drawing comparisons with ISPs in China, Ireland, and Nigeria to understand the variations in legal obligations and practices across different jurisdictions.

The research question delves into how the existing legal and regulatory frameworks in South Africa shape the operations and liabilities of ISPs, particularly in the context of cybercrime and content regulation. Understanding how these laws effectively deter cybercrimes, protect user privacy, and uphold freedom of expression is imperative. Moreover, the research seeks to unravel the complexities of implementing these laws, considering the technological advancements, and evolving nature of the Internet.

In the global context, this research will examine China, Ireland, and Nigeria's legal systems and internet governance models, providing a comparative analysis of their approaches to ISP regulation. This comparison aims to identify best practices, innovative solutions, and potential pitfalls in regulating ISPs, offering valuable insights that could be applied to the South African context.

The study will also analyze the impact of ISP regulation on various stakeholders, including consumers, the government, and the ISPs themselves. It will explore the balance between regulatory compliance and the ISPs' need to remain competitive and innovative. Additionally, the research will consider the ethical implications of ISP regulation, particularly regarding user privacy, data protection, and the right to information.

The detailed research questions are listed as follows:

- **Legal Framework and ISP Liability**: How do the current legal and regulatory frameworks in South Africa govern the operations and liabilities of ISPs, especially concerning cybercrime and online content?
- **Comparative Legal Analysis**: How do the legal systems and internet governance models in China, Ireland, and Nigeria differ from South Africa regarding ISP regulation, and what lessons can be learned from these jurisdictions?

- **Effectiveness of Legislation**: How effective are the existing laws in South Africa in achieving their intended objectives of deterring cybercrime, protecting user privacy, and upholding freedom of expression?
- **Impact on Stakeholders**: What are the implications of ISP regulation for consumers, the government, and ISPs regarding rights, responsibilities, and business operations?
- **Technological and Ethical Considerations**: How do technological advancements and ethical concerns influence the regulation of ISPs, and what challenges do these factors pose for effective governance?

Addressing these questions aims to construct a comprehensive framework to guide policy and legal reforms, ensuring that South Africa's ISP regulation is effective and equitable, keeping pace with global trends and technological innovations.

1.7 METHODOLOGY

In designing the methodology for this research, the researcher adhered to a qualitative desktop research approach.

1.7.1 RESEARCH DESIGN

Adhering to the interpretivist research philosophy,[115] this study employs a qualitative desktop research design, an approach meticulously selected for its appropriateness in delving into the intricacies of legal and regulatory frameworks that govern ISPs. This design is adept at unravelling the complexities inherent in the multifaceted domains of ISP operations, liability, and the socio-legal environment in which these entities function. The qualitative methodology facilitates an interpretive analysis of existing literature and documentary sources. This approach is conducive to gaining a comprehensive

[115] BRM "Interpretivism (interpretivist) Research Philosophy" https://research-methodology.net/research-philosophy/interpretivism/ (Date of use: 27 December 2023).

understanding of the statutory and regulatory nuances that define the ISP landscape and allows for extracting rich, contextual insights from various legal documents, policy papers, and scholarly articles.

In executing this design, the research leans heavily on systematically reviewing and synthesizing relevant information from many sources. This includes, but is not limited to, legal statutes, judicial decisions, government policy documents, and authoritative academic writings. Such a method ensures the research is grounded in a robust body of existing knowledge, providing a solid foundation for new insights and understandings. The choice of a desktop research methodology underscores the importance of a comprehensive and meticulous approach to data collection, ensuring that the research captures the most relevant and current information available in the public domain.[116]

Importantly, this research design aligns with the interpretivist paradigm by prioritizing the context and meaning behind the data gathered. This approach is not merely about aggregating data but rather about interpreting it to reveal underlying themes, patterns, and narratives.[117] Such an approach is vital in a dynamic and contextually dependent field such as internet governance and ISP regulation, where legal principles and policies are often deeply intertwined with technological, economic, and societal factors.

By adopting this qualitative desktop research design, the study is well-positioned to provide a nuanced and in-depth analysis of the role and liability of ISPs. It allows for a critical examination of how different jurisdictions approach ISP regulation, the challenges, and opportunities these entities face, and the impact of these factors on various stakeholders, including consumers, governments, and the ISPs themselves. This methodology is not just about gathering information; it's about understanding the stories behind the data, the narratives shaping ISP regulation, and the many factors influencing these narratives.

---

116 BRM "Interpretivism (interpretivist) Research Philosophy" https://research-methodology.net/research-philosophy/interpretivism/ (Date of use: 27 December 2023).

117 Pandey & Pandey 2021: 19.

1.7.2 DATE COLLECTION: DESKTOP RESEARCH

The data collection process for this study is meticulously structured around a comprehensive desktop literature review. This method is pivotal in collating and synthesizing various information sources[118] relevant to ISPs and their regulatory landscapes. This approach involves a detailed and systematic examination of various textual materials that provide insights into the legal, regulatory, and operational facets of ISPs. The literature review is not merely a collection of existing information but a critical appraisal and synthesis of various sources[119] to construct a coherent understanding of ISP liability and regulations across different jurisdictions.

The array of sources reviewed encompasses a broad spectrum of materials. This includes academic articles from peer-reviewed journals, which provide theoretical frameworks and empirical findings relevant to ISP operations and regulations. Legal documents such as statutes, legislative debates, and regulatory guidelines are integral to understanding the legal frameworks within which ISPs operate. Policy papers, especially those published by governments and regulatory bodies, offer insights into the intentions, implementations, and impacts of laws and regulations concerning ISPs.

Case law analysis forms a crucial part of the data collection process. By reviewing judicial decisions from South African, Chinese, Irish, and Nigerian courts, the research gains insights into the practical application of laws, the interpretation of legal statutes in real-world scenarios, and the judicial perspective on ISP liability issues. This literature review aspect is vital in jurisdictions where case law significantly influences legal interpretations and practices.

Furthermore, the literature review extends to governmental and non-governmental reports, which can provide empirical data, policy analyses, and evaluations of ISP regulations and their societal impacts. White papers, position statements from industry

[118] Pandey & Pandey 2021: 119.
[119] Newman & Gough 2020: 12.

bodies, and public consultations also form part of the reviewed material, offering a perspective on the stance and responses of ISPs and other stakeholders to regulatory changes and challenges.

The inclusion of multiple jurisdictions – South Africa, China, Ireland, and Nigeria in this desktop research allows for a comparative analysis that is both rich and diverse. Each jurisdiction offers a unique legal and socio-economic context, which, when compared, provides a more holistic understanding of ISP liability. This comparative approach enables the identification of commonalities and differences[120] in ISP regulation, shedding light on various models of Internet governance and their effectiveness.

1.7.3 SOURCES OF DATA

1.7.3.1 PRIMARY SOURCES

Primary sources form the bedrock of the study, offering direct insights into the legal and regulatory frameworks that govern ISPs. These include:

1. **Legislation**: National laws and statutes specifically address ISPs, internet governance, cybercrime, data protection, and digital rights. This research will examine the texts of relevant laws to understand the legal obligations and protections afforded to ISPs in different jurisdictions.

2. **Statutory Regulations**: Detailed regulatory guidelines and directives issued by government agencies or regulatory bodies that oversee ISP operations. These documents often provide practical applications of legislative principles and are crucial to understanding how ISPs are expected to comply with the law.

3. **Case Law**: Judicial rulings and court decisions pertaining to ISP liability and related internet governance issues. Analysis of case law will reveal how laws are

[120] Mishra & Alok 2022: 28.

interpreted and applied in real-world scenarios, providing valuable insights into legal precedents and the judiciary's perspective on ISP-related matters.

4. **Governmental Reports**: Official reports from government investigations, legislative studies, or commissions that provide analyses and recommendations on ISP regulation and internet policy. These reports often contain empirical data and expert insights, illuminating the government's viewpoint and policy intentions.

1.7.3.2 SECONDARY SOURCES

Secondary sources complement the primary data by providing interpretations, critiques, and broader contexts. These sources include:

1. **Academic Literature**: Scholarly articles, research papers, and books that discuss internet governance, ISP liability, and cyber law. Academic literature offers theoretical frameworks, empirical research findings, and critical analyses essential for understanding ISP regulation's complexities and the broader implications for society and technology.

2. **Policy Analyses**: In-depth analyses of ISP-related policies by think tanks, research institutes, and policy groups. These analyses often include evaluations of policy effectiveness, comparisons of different regulatory approaches, and recommendations for future policy directions.

3. **Expert Commentaries**: Articles, opinion pieces, and interviews with experts in internet governance, law, and technology. These commentaries provide professional insights, critiques of current policies, and predictions about future trends in ISP regulation.

4. **International Guidelines and Frameworks**: Documents from international organisations, such as the United Nations or the European Union, provide guidelines or frameworks for Internet governance and digital rights. These

sources help us understand global norms and standards that influence national ISP regulations.

The research aims to build a comprehensive and multi-faceted understanding of ISP liability and regulation across different legal and socio-economic contexts by utilising this diverse range of primary and secondary sources. This approach ensures a well-rounded analysis, incorporating various perspectives and interpretations.[121]

1.7.4 DATA ANALYSIS

In qualitative desktop research, data analysis is critical in distilling a wide range of information into meaningful insights. In this study on ISP liability and regulation, data analysis will be executed through a meticulous process of thematic analysis.

As a method, thematic analysis is particularly suitable for qualitative research involving diverse data sources, such as legislation, case law, academic articles, and policy papers.[122] This method enables the researcher to systematically sift through and categorize the data, thereby identifying recurring patterns, themes, and notable variances. The process begins with carefully reading and re-reading the collected data, allowing for an immersive engagement with the content. This immersion is crucial for recognizing subtle nuances and underlying themes that might not be immediately apparent.[123]

Once an initial familiarity with the data is established, the next step involves generating initial codes. This coding process, a foundational step in thematic analysis, involves labelling data segments with tags that summarize their core content or meaning. These codes serve as building blocks for the subsequent stages of analysis.[124]

---

121 Mishra & Alok 2022: 23.
122 Kumar 2019: 12.
123 Mishra & Alok 2022: 32.
124 Quinlan et al. 2019: 88.

Following coding, the study will progress to the theme development phase. The initially generated codes are examined and grouped based on their interrelationships, forming potential themes. This phase requires a higher level of abstraction, as it moves beyond mere description to interpret the significance of the patterns and connections within the data. The themes that emerge at this stage are not just common topics but represent deeper insights into the regulatory frameworks, operational challenges, and stakeholder perspectives regarding ISP liability.[125]

The next stage involves reviewing and refining the identified themes. This entails returning to the original data set to ensure that the themes accurately capture the essence of the data.[126] Themes may be split, combined, or discarded based on their coherence and relevance to the research objectives. This iterative process ensures that the final set of themes offers a comprehensive and accurate data representation.[127]

Once the themes are finalized, the study moves to the reporting phase, where the findings are narrated in a coherent and accessible manner. This involves describing each theme and interpreting their significance in the context of the research questions. The research aims to convey the complexities and intricacies of ISP regulation and liability, providing a nuanced understanding of the topic.

Throughout the data analysis process, the principles of systematic reviews play a crucial role. These principles emphasize the importance of a comprehensive and unbiased approach, methodological process transparency, and finding replicability.[128] Adhering to these principles ensures that the data analysis is rigorous but also credible and trustworthy.

125 Mishra & Alok 2022: 24.
126 Quinlan et al. 2019: 88.
127 Quinlan et al. 2019: 88.
128 Newman & Gough 2020: 9.

1.7.5 CHAPTER OVERVIEW

The research presents an overview of ISPs in South Africa and comparative jurisdictions, concentrating on their role and liability. The research is presented in seven chapters to wit:

Chapter One focuses on key terms which are central to the research. The researcher surveys the problem statement as well as the underlying research questions. Chapter One further presents the rationale for the choice of comparative jurisdictions as well as the content of each chapter.

Chapter Two contextualises ISPs and their development in the global law of the internet. The researcher departs from a non-jurisdictional detailed historical overview of the development of ISPs and then contextualises their place in the international legal sphere. The researcher also details the current challenges for and around ISPs in general.

Chapter Three focuses on the role and liability of ISPs in South Africa, focusing on the Constitution of the Republic of South Africa, 1996,[129] relevant legislation, case law and statutory interpretation.

Chapter Four presents a comparative overview of the role and liability of ISPs in China, focusing on the relevant constitutional provisions, national legislation, and judicial interpretation.

Chapter Five presents a comparative overview of the role and liability of ISPs in Ireland, focusing on the relevant constitutional provisions, national legislation, and judicial interpretation.

Chapter Six presents a comparative overview of the role and liability of ISPs in Nigeria, focusing on the relevant constitutional provisions, national legislation, and judicial interpretation.

Chapter Seven summarises the research findings and presents recommendations and conclusions for South Africa.

---

[129] Hereinafter referred to as the Constitution.

1.7.6 CHOICE OF COMPARATIVE JURISDICTION

Deutch opines:

> The differences, which we perceive in certain aspects of any two events, are perceived against a background of similarity with others, and so is the relative uniqueness of the event. We call an event unique if it is similar in every few aspects or dimensions, and different in very many from others. Without attempting comparison, how could we know that something was unique? If something were truly unique in any aspect, how could we discuss it? We should have no words for it. We could only talk about its negatives, calling it ineffable, un-measurable and so on, and then we would be very close to magic or religion and very far away from science.[130]

The above view of the value of differences and similarities is essential to any research. This research focuses on procedural similarities and differences between ISPs in South Africa, China, Ireland, and Nigeria through the lens of their role and liability. The comparative characteristics of each of the proposed jurisdictions will be thoroughly examined. The researcher submits that the role and liability of ISPs are best categorised by reviewing certain aspects of the underlying legal system in which they operate.

The above factors influenced the choice of comparative jurisdictions selected for the research.

1.7.6.1 THE PEOPLE'S REPUBLIC OF CHINA

With its unique internet governance model and legal framework, China presents a fascinating case study in understanding the role and liability of ISPs within a distinct regulatory and socio-political context. This overview will cover key aspects of China's approach to internet regulation, ISP responsibilities, and the broader implications for cyber governance. China's approach to internet governance is characterized by stringent state control and censorship, often termed the "*Great Firewall of China*." The Chinese government maintains tight control over online content, and ISPs are required to comply with strict regulatory requirements. The government justifies this control by

[130] Deutch 2001: 6.

saying it is necessary to maintain social stability, national security, and cultural values. The legal framework governing ISPs in China is robust and comprehensive. The Cybersecurity Law of 2017 is a crucial legislation that outlines the responsibilities of ISPs in ensuring cybersecurity and safeguarding national cyberspace sovereignty. ISPs must implement technical measures to prevent the transmission of banned content, monitor and report on cybersecurity incidents, and assist in legal investigations.

Under Chinese law, ISPs are significant in content monitoring and censorship. They must establish systems for monitoring and reporting prohibited content, including politically sensitive information, pornography, and content threatening national security. Failure to comply with these regulations can result in severe penalties, including revocation of business licenses and financial fines. ISPs in China are also mandated to authenticate the identity of their users. This involves real-name registration policies, making it easier for authorities to track online activities and enforce laws against online misconduct.

China's approach to cybersecurity emphasizes protecting critical information infrastructure. ISPs operating in critical sectors, such as telecommunications, finance, and public services, are subject to heightened security requirements. They must undergo regular security assessments and report any vulnerabilities to the authorities. Data protection is another critical aspect of ISP regulation in China. The Personal Information Protection Law (PIPL), enacted in 2021, places stringent controls on data collection, processing, and storage, aligning with global trends in data protection.

China's model of Internet governance and ISP regulation poses several challenges. The censorship practices have been criticized for stifling freedom of expression and limiting access to information. Moreover, the extensive obligations placed on ISPs for content control and surveillance raise concerns about privacy and the ethical implications of such surveillance. From a global perspective, China's approach to ISP regulation offers insights into how Internet governance can be tailored to meet specific national

objectives. However, it also highlights the potential trade-offs between state control and individual freedoms in cyberspace.

1.7.6.2 IRELAND

Ireland's approach to regulating ISPs and their role in the digital ecosystem presents a contrasting picture to countries like China, especially given its position within the European Union (EU) and its commitment to upholding EU directives and regulations. This discussion aims to encapsulate the Irish framework for ISP liability, its alignment with EU policies, and the resulting implications for Internet governance. Ireland's internet regulation landscape is primarily shaped by its adherence to EU laws and regulations, which tend to emphasize the protection of user privacy, data protection, and the free flow of information. Irish ISPs operate within a legal environment that balances these EU mandates with national interests. This approach significantly differs from the more controlled and censored regimes in countries like China.

In Ireland, ISPs are seen as intermediaries, a status that offers them certain protections under the EU's E-Commerce Directive. This directive stipulates that ISPs are not liable for the content they transmit, host, or store, provided they are unaware of its illegal nature or act expeditiously to remove it once they become aware. This "*mere conduit*" principle ensures that ISPs are not unduly burdened with monitoring all content that passes through their networks. This starkly contrasts the stringent monitoring requirements placed on ISPs in China.

However, this does not mean that ISPs in Ireland are free from obligations. They must adhere to various legal requirements, particularly data retention and law enforcement cooperation. The European Union's General Data Protection Regulation (GDPR) has significant implications for ISPs operating in Ireland. Under GDPR, ISPs, like all entities processing personal data, must ensure the security of such data and uphold users' privacy rights. This places a significant emphasis on the ethical handling of user data, transparency in data processing activities, and the implementation of robust cybersecurity measures.

Another critical aspect of Ireland’s approach to internet regulation is the focus on cybersecurity. ISPs are encouraged and sometimes mandated to implement robust cybersecurity measures to protect their infrastructure and users. The National Cyber Security Strategy outlines the government's approach to enhancing the cybersecurity ecosystem, promoting collaboration between the state, ISPs, and other stakeholders.[131] This collaborative approach aims to bolster Ireland's defences against cyber threats, a concern that has become increasingly paramount in the digital age.

The Irish model also reflects a nuanced understanding of the digital divide and the need for inclusive access to internet services. Efforts to expand broadband connectivity, especially in rural and underserved areas, are part of broader government initiatives to ensure equitable access to digital resources. This aligns with the European Digital Agenda, which aims to foster a digitally inclusive society.

Intellectual property rights and the battle against digital piracy are other areas where Irish ISPs have specific roles. The balance between protecting copyright and ensuring user freedoms is delicate, and Ireland has seen its share of legal challenges in this domain. The result has been the development of legal precedents and practices that attempt to respect both content creators' rights and internet users' freedoms. The role of ISPs in content regulation, while not as stringent as in countries like China, is still significant. There have been instances where Irish ISPs have been required by court orders to block access to certain websites involved in copyright infringement. These cases illustrate the complex role ISPs play in navigating legal and ethical considerations while providing internet services.

Irish ISPs face challenges like ensuring compliance with evolving EU regulations, addressing cybersecurity threats, and balancing between being conduits of information and gatekeepers against illegal content. The rapidly changing technological landscape poses continuous challenges in infrastructure development and adaptation to new

[131] The National, "Top 12 Cyber Crime Trends to Watch for in 2023," https://www.thenationalnews.com (Date of use: 9 Jauary 2024).

consumer demands and expectations. On the international front, Ireland's status as a hub for many multinational tech companies, including significant ISPs and internet companies, adds another layer of complexity. This positions Ireland uniquely in global discussions on internet governance, data protection, and digital rights, influencing its approach to ISP regulation.[132]

1.7.6.3 NIGERIA

Nigeria, Africa's largest economy and one of its most populous countries, presents a unique case in studying ISPs and their regulation. The country's approach to ISP liability and internet governance reflects its socio-political context, economic ambitions, and the challenges of balancing regulatory oversight with the promotion of digital inclusivity and freedom.

In Nigeria, the regulation of ISPs is influenced by a mix of national ambitions for technological advancement, the need for economic growth through digitalization, and concerns over security, privacy, and moral values.[133] The Nigerian government has been proactive in developing policies aimed at harnessing the potential of the Internet for economic development while also seeking to curb online malpractices.

The Nigerian Communications Commission (NCC) plays a pivotal role in regulating ISPs. The NCC's mandates include ensuring fair competition, quality service, and the protection of subscriber interests. One key aspect of NCC's regulation is expanding internet access. Nigeria has made significant strides in increasing internet penetration, with mobile internet playing a dominant role. However, the challenge remains to make this access equitable and to ensure that it contributes positively to socio-economic development.

Nigerian ISPs operate under regulations that require them to ensure network security and integrity. They are also tasked with combating cybercrimes, which have increased.

---

132 Dharmawan et al. 2019: 3178.
133 Ifonlaja 2023: 27.

The Cybercrimes Act of 2015 marked a significant step in Nigeria's efforts to address online criminal activities. Under this Act, ISPs must keep logs of all subscriber activities and provide them to law enforcement agencies upon request. This places a considerable responsibility on ISPs to monitor and report suspicious activities, striking a balance between user privacy and security needs.

The Act also makes provisions for offences such as cyberstalking and cyberbullying, reflecting societal concerns over the impact of the internet on social norms and values. ISPs are thus not just technical service providers but also gatekeepers against online harassment and abuse.

Data protection is another crucial area. The Nigeria Data Protection Regulation (NDPR), introduced in 2019, sets guidelines for data processing and handling, placing obligations on ISPs to protect user data. This regulation aligns with global trends in data protection, mirroring aspects of the EU’s GDPR. Despite these regulatory efforts, Nigerian ISPs face infrastructure, service quality, and challenges caused by the digital divide. The disparity in internet access between urban and rural areas remains a significant issue. There is also the challenge of frequent internet shutdowns, often instituted by the government in response to security concerns or to prevent misinformation during elections. These shutdowns raise questions about the balance between state security and freedom of expression.

Intellectual property rights and digital piracy are ongoing concerns in Nigeria. ISPs are often in a tricky position, navigating between protecting content creators' rights and ensuring open access to digital content. In terms of international perspective, Nigeria's stance on internet governance and ISP regulation is crucial, given its influence in the African continent. Nigeria's approach reflects an African perspective in global discussions on internet governance, balancing regional socio-economic realities with the global digital ecosystem's demands.

1.8 RESEARCH LIMITATIONS

The research aims to provide a comprehensive understanding of the legal frameworks and operational challenges faced by ISPs. However, as with any research endeavour, it encounters several limitations that might impact its findings and interpretations. Recognizing these limitations is crucial for contextualizing the conclusions and guiding future research. The limitations are highlighted below:

a) **Geographic and Cultural Specificity**: The study primarily focuses on South Africa, with comparative analyses involving China, Ireland, and Nigeria. While this provides a broad spectrum of legislative environments and ISP practices, the findings may not be fully generalizable to countries with diverse cultural, economic, or political contexts. The uniqueness of each jurisdiction's legal system and Internet governance policies can lead to conclusions specific to these countries and may not apply universally.

b) **Dynamic and Evolving Field**: Internet governance and ISP liability rapidly evolve, with modern technologies, policies, and user behaviours continually emerging. This fluidity means that the study's findings might become outdated quickly, necessitating continual updates and revisions to maintain relevance.

c) **Access to Data**: While the study relies on both primary and secondary data sources, there might be limitations in accessing comprehensive data, especially proprietary information from ISPs or detailed legal case studies. Some ISPs may be reluctant to share sensitive operational details, and legal proceedings may be subject to confidentiality constraints. This could limit the depth of analysis, particularly in the areas of ISP internal policies and the specifics of legal enforcement.

d) **Subjectivity in Analysis**: The researcher’s perspective and understanding could influence the analysis and synthesis of legal texts, leading to interpretations that might not fully capture the nuances of perspectives or legal intricacies. To mitigate

this limitation, the researcher continuously reflected on her role and position and sought feedback and criticism from her supervisor.

e) **Legal Complexity and Interpretation**: The study navigates complex legal landscapes involving different jurisdictions. Interpreting legal statutes, case law, and regulatory policies requires a nuanced understanding of legal language and principles, which can be subject to different interpretations. The complexity of legal analysis poses a challenge, especially in ensuring that interpretations accurately reflect the intent and application of laws in each jurisdiction.

f) **Language and Translation**: The study involves analyzing documents and laws from various countries, some of which may not be in English. Although translations might be used, there is always the potential for nuances to be lost in translation, which could affect the accuracy of the legal analysis.

g) **Reliance on Publicly Available Information**: The study depends on publicly available sources, including academic literature, legal documents, and public records. This reliance might overlook internal policy documents of ISPs or confidential legal settlements that could provide a different perspective on ISP practices and liabilities.

h) **Technological Limitations**: The rapidly changing technological landscape, including the advent of new digital communication and data transmission forms, poses a challenge in keeping the study's technological context current. New developments might emerge during the research, which are not accounted for in the study.

i) **Comparative Analysis Constraints**: While comparing different jurisdictions provides valuable insights, it also challenges aligning diverse legal and operational frameworks for a coherent analysis. The distinct nature of each jurisdiction's approach to ISP liability and internet governance might limit the depth of comparative analysis.

j) **Policy and Implementation Gap**: The study might highlight differences between policy (as written in law) and implementation (as practised), but fully exploring this gap is challenging due to the need for extensive field research and empirical data, which may be beyond the scope of this research.

1.9 PRELIMINARY CONCLUSION

In this chapter, the researcher introduced the research topic and contextualised the research approach, research question(s), and selected methodology. The content provided an overview of central research questions and contextualised them by defining significant research themes. The researcher explored the meanings of various terms in South African internet jurisprudence, legislation, and comparative jurisdictions by providing working definitions within the research context.

In chapter two, the researcher provides a brief overview of the development of the ISPs and then contextualises the contemporary approach with reference to international law.

CHAPTER TWO

INTERNET SERVICE PROVIDERS – HISTORICAL & CONTEXTUAL PERSPECTIVES

2.1 INTRODUCTION

This chapter contextualises the research topic and discusses ISPs via the historical and international law lens. The researcher provides a historical overview of the development of ISPs using a non-jurisdictional approach (where each specific jurisdiction is discussed in its relevant chapter) to demonstrate the changing philosophies that underpin their role and liability. The role and liability of ISPs are then highlighted in the international law sphere regarding international obligations to the United Nations, European Union, and African Union. The researcher further contextualises the contemporary challenges to ISPs and problematises their relation to content providers and end-users. The researcher aims to contextualise the role and liability of ISPs internationally and, after that, consider the impact on national legislation and functioning (chapters three to six) in South Africa and selected comparative jurisdictions.

2.2 INTERNET SERVICE PROVIDERS – HISTORICAL REFLECTIONS

The roots of ISPs can be traced back to the early days of the internet, with the establishment of Arpanet in the late 1960s.[134] Arpanet, a project funded by the United States Department of Defense, was the precursor to the modern internet.[135] However, it wasn't until the 1980s that the National Science Foundation (NSF) played a significant

---

134 Arpanet "Definition, history & significance" https://study.com/academy/lesson/arpanet-definition-historyquiz.html#:~:text=ARPANET%20was%20invented%20by%20a,ARPANET%20was%20born%20in%201969. (Date of use: 19 December 2023).

135 Arpanet "Definition, history & significance" https://study.com/academy/lesson/arpanet-definition-historyquiz.html#:~:text=ARPANET%20was%20invented%20by%20a,ARPANET%20was%20born%20in%201969. (Date of use: 19 December 2023).

role in shaping the internet landscape by creating NSFNET. This network provided the infrastructure for the first commercial ISPs to emerge.[136]

The 1990s witnessed a pivotal shift as the internet transitioned from a government and academic network to a commercially driven entity. The advent of the World Wide Web and the development of user-friendly browsers like Netscape Navigator fuelled the demand for internet connectivity. This surge in demand led to the emergence of commercial ISPs that could provide individuals and businesses with access to the internet.[137]

AOL, Prodigy, and CompuServe were among the early pioneers, offering dial-up internet services to a growing number of households. America Online (AOL) significantly popularised the Internet among the public, providing email services, chat rooms, and curated content.[138]

The late 1990s and early 2000s marked a shift from dial-up to broadband internet, transforming how people accessed and experienced the online world. Cable ISPs, leveraging existing cable television infrastructure, emerged as key players in delivering high-speed internet access to homes and businesses. Companies like Comcast and Time Warner Cable played pivotal roles in this transition, laying the groundwork for the broadband era.[139]

As technology continued advancing, Digital Subscriber Line (DSL) and fibre optic technologies emerged as alternatives to cable for high-speed internet delivery.

---

136 Arpanet "Definition, history & significance" https://study.com/academy/lesson/arpanet-definition-historyquiz.html#:~:text=ARPANET%20was%20invented%20by%20a,ARPANET%20was%20born%20in%201969. (Date of use: 19 December 2023).

137 Arpanet "Definition, history & significance" https://study.com/academy/lesson/arpanet-definition-historyquiz.html#:~:text=ARPANET%20was%20invented%20by%20a,ARPANET%20was%20born%20in%201969. (Date of use: 19 December 2023).

138 Arpanet "Definition, history & significance" https://study.com/academy/lesson/arpanet-definition-historyquiz.html#:~:text=ARPANET%20was%20invented%20by%20a,ARPANET%20was%20born%20in%201969. (Date of use: 19 December 2023).

139 Arpanet "Definition, history & significance" https://study.com/academy/lesson/arpanet-definition-historyquiz.html#:~:text=ARPANET%20was%20invented%20by%20a,ARPANET%20was%20born%20in%201969. (Date of use: 19 December 2023).

Telecommunication companies like Verizon and AT&T became prominent providers, offering DSL and fibre optic services to compete with cable ISPs. These technologies significantly increased internet speeds and bandwidth, allowing for more robust online experiences.[140]

In the 21st century, ISPs evolve, adapting to the increasing demand for faster and more reliable internet services. The rise of wireless technologies, such as 4G and 5G, has further expanded the reach of ISPs, enabling mobile internet access on a global scale. Additionally, the ongoing development of satellite internet services promises to bring connectivity to even the most remote areas.

2.3 INTERNET SERVICE PROVIDERS – PERSPECTIVES FROM INTERNATIONAL LAW

International law is essential for this research because it is directly relevant to South Africa. Regarding the South African Constitution,[141] a court must consider international law and may consider foreign law. A court must also interpret the Bill of Rights following the values of human dignity, equality, and freedom. The Constitution further provides that courts must prefer any reasonable interpretation of the legislation consistent with international law when interpreting any legislation.[142] For this reason, the researcher surveys international law applicable to the research topic and considers the obligations for comparative jurisdiction. The national law perspective is discussed in chapters three to six.

2.3.1 UNITED NATIONS

As of 2022, no specific United Nations (UN) convention exclusively governs ISPs. However, various international agreements, conventions, and treaties touch upon

140 Arpanet “Definition, history & significance” https://study.com/academy/lesson/arpanet-definition-historyquiz.html#:~:text=ARPANET%20was%20invented%20by%20a,ARPANET%20was%20born%20in%201969. (Date of use: 19 December 2023).

141 Section 39(1) of the Constitution.

142 Section 233 of the Constitution.

aspects related to the Internet, telecommunications, and the responsibilities of entities providing Internet services.

One significant instrument is the International Telecommunication Union (ITU), a specialized UN agency that addresses global telecommunications issues. While the ITU primarily focuses on telecommunications, its regulations and standards indirectly impact ISPs.[143] The ITU's International Telecommunication Regulations (ITRs) provide a framework for international telecommunication services, and though not specific to ISPs, they influence the broader telecommunications landscape.[144]

Another relevant document is the International Covenant on Civil and Political Rights (ICCPR), adopted by the UN General Assembly. The ICCPR addresses human rights, including freedom of expression and privacy, which are directly relevant to the operations of ISPs. Nation parties to the ICCPR are expected to uphold these rights, and any legislation or actions affecting ISPs within their jurisdictions should comply with these principles.[145]

Furthermore, the UN has recognized the importance of the Internet in achieving sustainable development goals (SDPs). Various UN bodies, including the UN General Assembly, have discussed the need for an inclusive, open, and secure cyberspace. While not forming a specific convention, these discussions emphasize the significance of international cooperation and the rule of law in the digital realm.[146]

While no UN convention exclusively governs ISPs, international agreements, especially those related to telecommunications, human rights, and sustainable development,

---

143 ITU "About the International Telecommunication Union" https://www.itu.int/en/about/Pages/default.aspx (Date of use: 9 December 2023).

144 ITU "About the International Telecommunication Union" https://www.itu.int/en/about/Pages/default.aspx (Date of use: 9 December 2023).

145 Council of Europe "The International Covenant on Civil and Political Rights" https://www.coe.int/en/web/compass/the-international-covenant-on-civil-and-political-rights (Date of use: 13 August 2023).

146 United Nations "Sustainable Development Goals" https://sustainabledevelopment.un.org/topics/sustainabledevelopmentgoals (Date of use: 13 January 2024).

collectively shape the global landscape in which ISPs operate.[147] The ongoing discussions and developments in international forums underscore the importance of a collaborative and rights-respecting approach to Internet governance.

2.3.2 EUROPEAN UNION

The EU legislature watered down the effect of Directive 2004/48 and Directive 2001/29 by introducing laws that limited the liability of ISPs. Article 15(1) of the 2000 Electronic Commerce Directive[148] limits the legal effect of the injunctions imposed by national courts.

Article 15(1) of the directive bars Member States from implementing laws, policies, and rules that force service providers to monitor data that internet users are transmitting through their networks. Furthermore, Article 15(1) bars Member States from implementing rules, laws, and policies that require service providers to monitor the traffic flowing through their networks for illegal activity.[149]

It has been argued that Article 15(1) of the Directive limits the effectiveness of the directives, giving internet users and courts the right to institute legal action against ISPs. The wording in Article 15(1) of the Directive restricts the laws and policies of Member States to matters related to the prevention of the infringement of intellectual property rights.[150]

If the matter goes beyond prevention and into monitoring the data that internet users are transmitting through the ISPs' networks, the EU Court will rule that the law, rule, or policy is incompatible with the provisions of EU laws. Commentators have also argued that Article 15(1) of the Directive prevents national legislatures and the courts from

147 ITU "About the International Telecommunication Union" https://www.itu.int/en/about/Pages/default.aspx (Date of use: 9 December 2023).
148 Article 15(1) Directive 2000/31/EC.
149 Article 15(1) Directive 2000/31/EC.
150 Article 15(1) Directive 2000/31/EC.

implementing rules, laws, or policies that impose onerous obligations on the service providers.[151]

For instance, a rule requiring service providers to monitor their network for illegal activities would be onerous because it would force them to use costly programs. Implementing the systems that monitor the traffic on the site for unlawful activity would force the ISPs to move away from their core competence and focus on matters that are markedly different from their core objectives.

In addition to Directive 2000/31, Article 3 in the 2004 Electronic Commerce Directive offers further ground for limiting the liability of ISPs and other intermediaries. Article 3 of the Directive prohibits Member States from implementing rules, laws, and policies that impose costly, disproportionate, or unfair obligations on the service providers.[152]

Article 3(1) states that the measures implemented to safeguard intellectual property rights must be equitable, fair, cost-effective, reasonable, and timely.[153] Article 3(2) states that the remedies implemented to safeguard the interests of the holders of intellectual property rights should not undermine the interests of trade.[154] This provision warns the national legislatures and Member States against implementing rules that hinder the free movement of goods, services, and people.

The doctrine of the free movement of goods, services, and people is at the core of the EU Constitution.[155] Therefore, Article 3 requires municipal courts and municipal legislators to consider the principle of free movement of goods and services when implementing the laws that will punish intermediaries, like ISPs, to the extent that they undermine that principle.[156]

---

151 Article 15(1) Directive 2000/31/EC.
152 Article 3 of Directive 2004/48/EC.
153 Article 3 of Directive 2004/48/EC.
154 Article 3 of Directive 2004/48/EC.
155 Article 3 of Directive 2004/48/EC.
156 Article 3 of Directive 2004/48/EC.

Where a municipal court ruling or a national law violates the rule requiring States to implement policies, rules, and laws compatible with the Article on the Promotion of Trade, the EU Court has an obligation to set aside the ruling because it is incompatible with the EU laws.

Indeed, the EU courts have dealt with various cases in which they have struck down the national policies and laws that recommend punishments to the ISPs that have failed to respect the interests of intellectual property rights holders. Within the EU, the legislature and the courts have restricted Member States' ability to hold ISPs liable.[157] EU laws, particularly those concerning the free movement of goods and the right of companies to provide services, have imposed restrictions that make it hard for Member States to enact laws that impose strict liability on the ISPs. The EU Court of Justice has interpreted the laws on the free movement of goods and the right of companies to provide services, giving states the right to enact laws that regulate the ISPs. Still, those regulations must be within the EU's Regulations.

This position became apparent when the EU Court dealt with the *Scarlet Extended SA v SABAM* [158] and *SABAM v Netlog* cases.[159] The *Scarlet Extended* case arose in 2004 when *SABAM*, a Belgium-based management company that manages the copyright materials of music editors, composers, and authors, instituted a case against *Scarlet* (an ISP that offered internet services to third parties).

In its suit, in a Belgium Court, *SABAM* argued that *Scarlet*'s customers were infringing on the rights of its clients through their unauthorised download of copyrighted books, songs, and videos. *SABAM* argued that *Scarlet*'s failure to implement filtering mechanisms meant internet users could use peer-to-peer file-sharing software to illegally download copyrighted songs, books, and compositions.

---

157 Lewis 2010: 56.

158 *Scarlet Extended SA v Societe Belge des Auteurs, Compositeurs et Editeurs SCRL (SABAM)* (C-70/10) [2011] E.C.R. I-11959 (24 November 2011). Herinafter referred to as *Scarlet Extended.*

159 *SABAM v Netlog* C-360/10 (EU:C: 2012:85). Hereinafter the *Netlog* case.

SABAM urged the Belgian Court to impose an injunction against *Scarlet* and order the company to install filtering mechanisms that make it impossible for internet users to send, receive, or download copyrighted books and music. In 2007, the Belgian Court of First Instance agreed that *Scarlet's* failure to implement a filter showed that it was complicit in its customers' infringement of the protected copyrights.

In line with this, the Belgian Court ordered them to introduce filters and other measures undermining their customers' ability to send, receive, or download copyrighted songs and books.[160] *Scarlet* instituted an appeal with the Appeals Court in Brussels. However, the Appeals Court stayed the injunction and transferred the case to the European Court.[161]

The Appeals Court wanted the EU Court to make a preliminary ruling on the legality of the injunction by the court of first instance.[162] The Appeals Court sought to determine whether the court, in the first instance, complied with EU laws when it imposed an injunction on an ISP for the actions of the third-party individuals and the organisations that were using its site.

Furthermore, the Appeals Court sought to determine whether the Belgian National Court violated the EU laws by compelling the ISP to install filters and other measures preventing internet users from sending, receiving, or downloading copyrighted content.

The EU Court ruled that the injunction and the order compelling *Scarlet* to install the filters were incompatible with the EU laws. According to the EU Court, Article 15(1) of the EU Directive[163] prevents the National Courts (and the national legislatures of EU Member States) from imposing rules that compel ISPs to implement measures that allow them to monitor the data that the internet users transmit through their network.

160 *Scarlet* Extended.
161 *Scarlet* Extended.
162 *Scarlet* Extended.
163 EU Directive 2000/31.

The Court added that a ruling requiring the ISPs to implement the filters would violate the internet users' right to privacy and freedom of expression.[164] The Court argued that the rules requiring the ISPs to filter would violate these fundamental rights in two ways. First, they would violate fundamental rights by permitting the ISPs to monitor the messages and files the internet users transmit through their network. Secondly, the rules would violate fundamental rights by allowing the ISPs to regulate what internet users can read, watch, and share.

Based on the ruling in *Scarlet* and the outlined provisions, one can argue that EU Courts have rejected the attempts by the national legislature and governments to hold the ISPs accountable for the violations by third parties who use their networks.

The EU Courts and EU legislature hold such a view because of their perception that establishing strict obligations on the part of ISPs would violate the fundamental rights of the ISPs and the internet users.[165] The EU Courts and the legislature believe that Member States ought to strike a balance between making the ISPs liable and respecting the rights of the ISPs to conduct their business affairs, as well as the right of the internet users to their privacy.[166]

The courts and legislature believe that implementing the national rules and policies requiring the ISPs to implement a filtering system (that prevents third parties from violating the rights of copyright holders) would open doors for the ISPs to violate the internet users' right to privacy and freedom of expression.[167]

The ISPs would violate these fundamental rights by making monitoring the internet users' data sending, storing, and receiving easier.[168] They believe that implementing the policies that seek to hold the ISPs liable for violating third-party users would undermine

164 *Scarlet Extended.*
165 Lenaerts 2015: 11.
166 Jouanjan 2009: 877.
167 Jouanjan 2009: 877.
168 Jouanjan 2009: 877.

their ability to conduct their businesses within the EU.[169] The essence of these arguments is that the EU Courts and legislature believe that the imposition of liability on the ISPs (and other intermediaries) is only possible when one has balanced it against the need to protect the fundamental rights and freedoms of the internet users and the ISPs.

The EU Court provided a further illustration of the need for national courts and national legislatures to strike a balance between the rights of the holders of intellectual property rights and the fundamental rights and freedoms of EU nationals and companies which have invested in the EU.

In *SABAM v Netlog*,[170] *SABAM* (an organisation representing the intellectual property rights of musicians, authors, and other intellectual property rights holders within the EU) instituted a case against *Netlog* (a social media ISP). In this case, *SABAM* alleged that *Netlog* violated the intellectual property rights of its clients by allowing internet users to share, receive, and distribute copyrighted materials without the express consent of their owners.

In the suit, *SABAM* asked the Belgian Court to issue an order requiring *Netlog* to pay a fee to *SABAM* because it permits third parties to use its network to send and receive copyrighted files. In addition, *SABAM* asked the EU Court to order *Netlog* to stop the file-sharing practices of its website users.[171]

In response, *Netlog* filed a preliminary objection in which it asked the Belgian Court to suspend the proceedings until the EU Court had determined whether the imposition of a fee and the order on file sharing amounted to a violation of the provisions of EU Directives, as well the fundamental rights enshrined in the EU Constitution.[172] *Netlog* argued that imposing a fee and implementing filters would violate Directive 2004/48 and

169 Wu 2006: 269.
170 *Netlog*.
171 *Netlog*.
172 *Netlog*.

Directive 2001/29.[173] It also argued that the decisions would violate internet users' privacy and freedom of information rights.

Therefore, the issue for determination by the EU Courts was whether the fee and the injunction would violate the fundamental freedoms and the rights of internet users.[174] Persuaded by *Netlog*'s arguments, the EU Court issued an order preventing the Belgian Court from proceeding with the case. The EU Court held that national courts and legislatures ought to balance the interests of the copyright holders and the internet users.[175]

The EU Court argued that the national courts and legislature must balance the intellectual property rights of the holders and the fundamental rights and freedoms of internet users.[176] In particular, it argued that the measures taken to safeguard the interests of intellectual property holders should not infringe on internet users' freedom of expression and right to privacy.[177]

These arguments indicate that the EU Court regards the rights of copyright holders as subservient to the fundamental rights and freedoms of Internet users. Efforts by the national courts and the legislature to establish laws, policies, and rulings that purport to safeguard the rights of copyright holders will fail if they do not consider the rights and freedoms of internet users and ISPs.

The EU has enacted several laws that outline the extent of the liability of ISPs for violations committed by individuals and organisations using their networks to send or receive data. Regarding the liability of ISPs, the relevant laws are EU Directive 2004/48 and EU Directive 2001/29.

---

173 *Netlog*.
174 *Netlog*.
175 *Netlog*.
176 *Netlog*.
177 *Netlog*.

Article 8(3) directs Member States to implement policies and laws that make it easier for the holders of copyright and other intellectual property rights to request the courts to issue injunctions against the intermediaries in situations where third parties are using their networks to infringe on the rights of the holders of copyright and other intellectual property rights.[178]

Article 11 of the 2004 Directive has a similar provision. The Article directs all Member States of the EU to implement laws allowing the right holders to institute claims against individuals and organisations infringing their intellectual property rights. Furthermore, the Article directs Member States to expand the scope of the intellectual property infringement laws to include intermediaries whose networks provide opportunities to violate intellectual property rights.

The term "*intermediaries*" suggests that the EU legislature wants to cover various organisations, including ISPs. It means that the EU legislature intends to give Member States the power to enact laws that make it easier for holders of intellectual property rights to hold ISPs accountable whenever their omissions make it easier for intellectual property rights violations.

The issuance of injunctions against the ISPs and other subsidiaries implies that parties alleging intellectual property rights violations can ask the courts to end the violations and impose limitations that prevent the ISPs from engaging in additional infringements.

However, the EU legislature has watered down the effect of Directive 2004/48 and Directive 2001/29 by introducing laws that limit the liability of ISPs. Article 15(1) of the 2000 EC Directive[179] limits the legal effect of the injunctions imposed by national courts, as mentioned in the introduction of this subheading.

Article 15(1) of the directive bars Member States from implementing laws, policies, and rules that force service providers to monitor data that internet users are transmitting

[178] Article 8(3) of Directive 2001/29/EC.
[179] Article 15(1) Directive 2000/31/EC.

through their networks. Furthermore, Article 15(1) bars Member States from implementing regulations, laws, and policies that require service providers to monitor the traffic flowing through their networks for illegal activity.

Article 3(2) states that the remedies implemented to safeguard the interests of the holders of intellectual property rights should not undermine the interests of trade.

This provision warns national legislatures and Member States against implementing rules that hinder the free movement of goods, services, and people. The doctrine of the free movement of goods, services, and people is at the core of the EU constitution.[180] Therefore, Article 3 requires municipal courts and municipal legislators to consider the principle of free movement of goods and services when implementing the laws that will punish intermediaries, like ISPs, to the extent that they undermine that principle.[181]

Where a municipal court ruling or a national law violates the rule requiring States to implement policies, rules, and laws compatible with the Article on the Promotion of Trade, the EU Court must set aside the ruling because it is incompatible with the EU laws.

Indeed, the EU courts have dealt with various cases in which they have struck down the national policies and laws that recommend punishments to the ISPs that have failed to respect the interests of intellectual property rights holders. Within the EU, the legislature and the courts have restricted Member States' ability to hold the ISPs liable.[182]

---

180 William et al. "Freedom of connection – freedom of expression: The changing legal and regulatory ecology shaping the internet" 2010 http://www.milthailand.org/phocadownload/2011_Files/10_Oct/media/freedompercent20ofpercent20connectionpercent20freedompercent20ofpercent20expression.pdf (Date of use: 1 December 2016).

181 Tsai 2011: 402.

182 Lee et al. 2013: 406.

EU laws, particularly those concerning the free movement of goods and the right of companies to provide services, have imposed restrictions that make it hard for Member States to enact laws that impose strict liability on the ISPs.[183]

SABAM urged the Belgian Court to impose an injunction against *Scarlet* and order the company to install filtering mechanisms that make it impossible for internet users to send, receive, or download copyrighted books and music.

In 2007, the Belgian Court of First Instance agreed that *Scarlet*'s failure to implement a filter showed that it was complicit in its customers' infringement of the protected copyrights.

The Appeals Court wanted the EU Court to make a preliminary ruling on the legality of the injunction by the court in the first instance. The Appeals Court sought to determine whether the court, in the first instance, complied with EU laws when it imposed an injunction on an ISP for the actions of the third-party individuals and the organisations that were using its site.

Based on the ruling in *Scarlet* and the outlined provisions, one can argue that EU Courts have rejected the attempts by the national legislature and governments to hold the ISPs accountable for the violations by third parties who use their networks.

The EU Courts and the legislature believe that Member States ought to strike a balance between making the ISPs liable and respecting the rights of the ISPs to conduct their business affairs, as well as the right of the internet users to their privacy.[184]

However, the European Court of Human Rights (ECHR) rulings indicate that it has been willing to hold the ISPs and other intermediaries liable whenever the activities of third parties in networks run by these intermediaries lead to violating the fundamental rights and freedoms of EU citizens. The rulings of the ECHR suggest that it holds the view that it is possible to hold "*intermediaries*" responsible whenever third parties, using their

183 Dann & Haddow 2008: 222.
184 Lenaerts 2015: 15.

networks or sites, infringe on other people's rights. This became apparent in the case of *Delfi v Estonia*.[185]

In this case, the applicant company owned one of Estonia's largest Internet news portals. On its website, readers could post comments below the published articles anonymously and without prior registration. Although the applicant company could not edit or moderate such comments, it could remove them using a prior automatic word filtering system or by being alerted by readers. In 2006, the applicant published an article stating that a ferry company had changed its routes, causing ice break-ups at potential ice road locations. As a result, the opening of the roads – which were a cheaper and faster connection to the Estonian islands compared to the company's ferry services – had to be postponed for several weeks. Several comments containing personal threats and offensive language directed against the ferry company owner were posted below the article. The applicant company removed them some six weeks later at the insistence of the ferry company. The owner of the ferry company instituted defamation proceedings against the applicant company, which was ordered to pay EUR 320 in damages.

The ECHR held that it was possible to sue *Delfi* for the defamatory statements published on its internet site. The Court asserted that the complainants had a right to sue and seek compensation from *Delfi*. According to the ECHR, *Delfi* was able to evaluate the authenticity of the claims in the article before its publication.

The Court ruled that *Delfi* could evaluate and predict the defamatory content in the article and take all the measures needed to prevent its authors from publishing the article on its portal. In arriving at this conclusion, the Court compared *Delfi* to a publisher. The Court argued that it had a duty to evaluate the authenticity of the statements made in the article before its publication.

185 *Delfi v Estonia* Application No. 64569/09/ (hereinafter the *Delfi* case).

This ruling led to an intense debate. Human rights organisations felt that *Delfi's* categorisation as a publisher opened the doors for characterising all intermediaries as publishers.

Human rights organisations contended that the ECHR would be willing to hold ISPs and other intermediaries to account for the violations orchestrated by third parties using their internet portals and networks. The rights organisations added that the ruling would pave the way for intermediaries to violate the rights and freedoms of internet users by permitting intermediaries to monitor the messages they were sending, receiving, and storing. [186]

Interestingly, the ECHR ruled that *Delfi* was responsible for the defamatory content even though the applicant failed to identify the individuals who published the article. The facts of the case suggest that anonymous posters published the article. Therefore, it became difficult for *Delfi* to provide the identity of the individuals who authored the article and used the *Delfi* portal to disseminate its contents to the Estonian public.

Delfi argued that although it controlled and managed the portal, most of it was through an automated system developed to flag down defamatory or racist remarks. *Delfi* contended that implementing a system for editing all publications on the portal would force it to close its operations because it did not have the resources necessary to employ the workforce.

However, these arguments did nothing to persuade the judges of the ECHR. The judges ruled that *Delfi* had a duty to provide the measures necessary to prevent damage to the reputation of third parties, as it was running a professionally managed news portal.

The judges added that the anonymity of the article's authors could not excuse *Delfi* from its obligation to ensure that no articles published on its portal are injurious to the

[186] Lenaerts 2015: 11.

reputation of other individuals. The ECHR stated that its failure to satisfy this duty meant that the ruling of the Estonian Courts that *Delfi* was guilty of defamation ought to stand.

The Court argued that the ruling ought to be upheld, as it is a proportionate and justified restriction of *Delfi's* and other internet users in the country's freedom of expression. This argument demonstrates that the ECHR is ready to circumvent many of the restrictions that the European Court of Justice and the EU legislature implemented to protect the interests of ISPs and other intermediaries when necessary.

It suggests that the ECHR can implement specific measures to bring ISPs and other intermediaries to account whenever third parties use their websites to violate citizens' fundamental rights and freedoms. However, the issue that remains outstanding is whether the ECHR can make a ruling that safeguards the interests of Member States of the EU, especially when terrorists and other third parties are using the networks provided by ISPs to undermine their interests.

The possibility that terror groups and other third-party organisations can use the networks and systems provided by ISPs to undermine the government is genuine. Evidence from the recent USA election and the widespread "*ransomware*" attacks suggest that attacks targeting government institutions and the institutions essential to the functioning of the government are becoming rampant.

State agencies in North Korea, China, Israel, and Iran are now using hacking as a weapon against the States that they perceive as their enemies. Government institutions in the EU have fallen victim to these attacks. The negative impact of these attacks on government institutions raises the probability that one of the EU Member States will implement a policy, law, regulation, or measure holding ISPs and other intermediaries criminally liable for the attacks on government institutions.

Such a measure will put the government in the crosshairs of organisations that protect freedom of expression. Many organisations will refer to the European Court of Justice cases or the ECHR, arguing that it violates internet users' fundamental rights and

freedoms. These organisations may argue that the law undermines the right to privacy and freedom of expression, forcing ISPs and other intermediaries to filter information on their networks and monitor users' data.

Given the conflicting rulings by the ECHR and the European Court of Justice, it will be interesting to note how both courts will react to such a case in future. Future analysts may focus on the ECHR to assess whether it will rule that the privacy rights and freedom of expression infringements arising from such laws, rules, or measures are necessary to protect EU citizens' health and safety.

Future analysts could also train their eyes on the European Court of Justice to determine whether it will maintain its stance on the rules, measures, and laws that impose onerous conditions on ISPs and other intermediaries. The European Court of Justice has already held that such rules are unlawful because they undermine intermediaries' right to do business. It has also held that such laws and regulations are invalid because they violate the right of internet users to express themselves freely and privately.

The European Union has been actively working on regulating artificial intelligence (AI) through the proposed AI Act. The key point for the Act indicates:

i. Risk-based approach: The regulation categorises AI systems based on their potential risks, from unacceptable to minimal risk.
ii. Prohibited practices: Certain AI applications are banned, such as social scoring systems and manipulative AI.
iii. High-risk AI systems: These require strict oversight, including risk assessments, human oversight, and transparency measures.
iv. Transparency requirements: AI systems must be clearly labelled as such when interacting with humans.
v. Sanctions: Non-compliance can result in significant fines.
vi. AI Board: A European Artificial Intelligence Board will be established to facilitate implementation.

vii. Innovation support: The regulation aims to balance innovation with safety and ethical concerns.

The AI Act is still being finalized and implemented. Its goal is to create a harmonized approach to AI regulation across the EU while fostering innovation and protecting fundamental rights. At the time of writing the AI Act was not yet in force, and its status reflects as follows:

i. Provisional agreement: In December 2023, the European Parliament and Council reached a provisional agreement on the AI Act.
ii. Formal approval: The text was formally approved by the European Parliament in March 2024.
iii. Implementation timeline: The regulation is set to become fully applicable two years after its entry into force, with some provisions applying earlier.
iv. Current stage: The Act is in a transition period. It's expected to be published in the Official Journal of the EU and enter into force 20 days after publication.
v. Gradual implementation: Some parts of the Act, like the ban on prohibited AI practices, will apply earlier than others.
vi. Preparation period: Companies, governments, and other stakeholders are currently preparing for compliance.

The exact date when the AI Act will be fully operational depends on the final publication date, but it's expected to be fully applicable around 2026. However, its influence is already being felt as organizations prepare for compliance.

The European Union and Africa have quite different approaches to regulating AI, reflecting their distinct economic, technological, and political contexts. Below follows a comparison:

European Union:

i. Comprehensive framework: The EU has developed the AI Act, a detailed, legally binding regulation.

ii. Risk-based approach: Classifies AI systems based on risk levels, with stricter rules for higher-risk applications.
iii. Harmonized standards: Aims to create uniform rules across all EU member states.
iv. Focus on ethics and fundamental rights: Emphasizes protecting individual privacy and preventing discrimination.
v. Substantial resources: Significant financial and institutional resources dedicated to AI governance.
vi. Global influence: The EU's approach is likely to have a global impact due to the "Brussels effect."

Africa:

i. Diverse approaches: Regulation varies significantly between countries, with no continent-wide framework like the EU's.
ii. Focus on development: Many African countries prioritize AI adoption for economic development over strict regulation.
iii. Limited resources: Generally fewer resources available for creating and enforcing comprehensive AI regulations.
iv. Data protection laws: Some countries have implemented data protection laws that indirectly affect AI, but these aren't AI-specific.
v. Regional initiatives: Organizations like the African Union are working on guidelines, but these are not yet as comprehensive or binding as the EU's.
vi. Emphasis on inclusion: Many African AI initiatives focus on ensuring AI benefits are distributed equitably and reflect African values and needs.
vii. Capacity building: Significant effort is being put into building AI skills and infrastructure rather than creating regulatory frameworks.

Key differences:

1. Regulatory maturity: The EU's approach is more mature and comprehensive.
2. Economic context: Africa often prioritizes AI adoption for development, while the EU focuses more on managing risks of already widespread AI.

3. Resources: The EU has more resources to devote to AI governance.
4. Unity: The EU presents a more unified approach compared to the diverse strategies across African nations.

It's worth noting that the situation is evolving, with some African countries and regional bodies working towards more comprehensive AI governance frameworks. However, the approaches remain quite different from the EU's regulatory model. How the AI Act will effect ISPs remains to be seen.

2.3.3 AFRICAN UNION

Like the UN, the African Union (AU) does not have a specific convention or comprehensive framework dedicated solely to the governance of ISPs. However, the AU, recognizing the critical role of information and communication technologies (ICTs) in socio-economic development, has engaged in initiatives and discussions related to internet governance, digital infrastructure, and technology policies.[187]

The AU's Agenda 2063, a strategic framework for the continent's socio-economic transformation, includes aspirations highlighting the importance of leveraging technology for development. It includes building a robust digital economy, enhancing ICT infrastructure, and promoting innovation. While not explicitly focused on ISPs, these aspirations indirectly influence the environment in which ISPs operate.[188]

The AU has also been involved in discussions around cybersecurity, recognizing the importance of securing digital spaces.[189] Cybersecurity is intricately linked to the

[187] African Union "The Digital Transformation Strategy for Africa (2020-2030) https://au.int/en/documents/20200518/digital-transformation-strategy-africa-2020-2030 (Date of use: 12 December 2023).

[188] African Union " Agenda 63: The Africa We Want" https://au.int/en/agenda2063/overview (Date of Use: 3 January 2024).

[189] African Union "The Digital Transformation Strategy for Africa (2020-2030) https://au.int/en/documents/20200518/digital-transformation-strategy-africa-2020-2030 (Date of use: 12 December 2023).

operations of ISPs, and any efforts to enhance cybersecurity within the AU member states could impact the policies and practices of ISPs operating in the region.

In addition, regional economic communities within Africa, such as the Economic Community of West African States (ECOWAS) and the East African Community (EAC), have specific initiatives and agreements related to ICTs and ISPs. These regional bodies often collaborate with the AU to harmonize policies and promote regional integration.[190]

Despite the lack of specific regulations relating to ISPs, the AU has been actively involved in initiatives to enhance digital infrastructure and connectivity across the continent. One project that aligns with the AU's efforts to improve internet infrastructure is the African Internet Exchange System (AXIS) project.[191]

The AXIS project, supported by the AU Commission, aims to strengthen the Internet ecosystem in Africa by promoting the establishment and interconnection of Internet Exchange Points (IXPs) across the continent.[192] IXPs facilitate internet traffic exchange between networks, including ISPs, content providers, and other entities.

By promoting the development of IXPs, the AXIS project seeks to reduce the reliance on international links for internet traffic, thereby improving network efficiency, reducing latency, and lowering costs for ISPs.[193] This initiative aligns with the broader goals of the AU's Agenda 2063, which includes aspirations related to building a robust digital economy and enhancing ICT infrastructure.

190 Nyinevi & Ayalwe 2022: 101.
191 African Union "African Internet Exchange System (AXIS) Project Overview" https://au.int/en/african-internet-exchange-system-axis-project-overview (Date of use: 22 June 2023).
192 African Union "African Internet Exchange System (AXIS) Project Overview" https://au.int/en/african-internet-exchange-system-axis-project-overview (Date of use: 22 June 2023).
193 African Union "African Internet Exchange System (AXIS) Project Overview" https://au.int/en/african-internet-exchange-system-axis-project-overview (Date of use: 22 June 2023).

In the context of the AU's engagement with the AXIS project, it becomes evident that it recognizes the importance of creating an environment conducive to the effective operation of ISPs. By fostering regional interconnection and collaboration through initiatives like AXIS, the AU contributes to developing a more resilient and interconnected internet infrastructure in Africa.

2.4 CONTEMPORARY CHALLENGES FOR THE INTERNET SERVICE PROVIDERS

2.4.1 LEGAL INFRASTRUCTURE IN AFRICA IS INEFFECTIVE IN PROTECTING CONSUMERS

Like ISPs and content providers, African governments' and other policymakers' responses have been slow. Despite high internet usage rates and the unprecedented use of social media technologies, African governments such as Nigeria, South Africa, and Egypt have yet to enact a practical framework of cyber laws to govern the interaction between internet users, content providers, and ISPs.

Many existing laws do not provide the safeguards to protect the government, consumers, and other stakeholders from the adverse consequences of interaction between internet users, content providers, and ISPs.

Consumers have faced a significant challenge from the spike in cybercrime rates. Statistics suggest that the African countries with the highest rates of internet access are also the countries with the highest instances of cybercrime. According to the statistics, Nigeria annually loses over US$ 450 million due to cybercrime.[194]

A report published by the Nigerian Senate suggests that the country annually loses US$ 450 million to attacks on its ICT infrastructure and ICT space. The report indicates that

[194] Adebayo http://dailypost.ng/2017/03/08/nigeria-losses-n127b-annually-cyber-crimebuhari percentE2percent80percent8E/ (Date of use: 22 July 2017).

over 70 per cent of the money lost arises from hacking-related crime alone.[195] Statistics suggest that the money that the country loses to cybercrime is equivalent to 0.8 per cent of its Gross Domestic Product (GDP). In addition, the statistics indicate that the perpetrators of cybercrime in Nigeria are Nigerians, with the data indicating that 7.5 per cent of the world's leading hackers are Nigerians. In many of these cybercrime cases, security agencies cannot act to safeguard consumers from the attacks nor help consumers recover their money. These security agencies lack the human, financial, and technological resources to investigate such crimes.[196]

In 2015, a Report published by Nigeria's Information Security Society (ISS) confirmed this state of affairs by stating that more than 25 per cent of the country's cybercrimes remain unresolved.[197] In the Report on the Deliberations in the Nigerian Senate, Hanibol Goitom argues that the Head of the Senate Committee on Cybercrime (SCC) has suggested that hackers and other cyber-criminals were thriving in the country because of a significant gap in the country's laws.[198]

He argues further that the country's ICT infrastructure and cyberspace were so porous that cyber-criminals orchestrated cyber-attacks without worrying about the possibility of arrest.[199] The Head of the SCC argued that there was a need for the Senate to enact laws that provide security agencies and the government with greater control over the security of the ICT infrastructure and cyberspace.[200]

---

195 Umoru http://www.vanguardngr.com/2017/05/450m-lost-cyber-crime-nigeria-senate/ (Date of use: 22 July 2017).

196 Adebayo http://dailypost.ng/2017/03/08/nigeria-losses-n127b-annually-cyber-crimebuhariper centE2percent80percent8E/ (Date of use: 22 July 2017).

197 Adebayo http://dailypost.ng/2017/03/08/nigeria-losses-n127b-annually-cyber-crimebuhariper centE2per cent80per cent8E/ (Date of use: 22 July 2017).

198 Umoru http://www.vanguardngr.com/2017/05/450m-lost-cyber-crime-nigeria-senate/ (Date of use: 22 July 2017).

199 Umoru http://www.vanguardngr.com/2017/05/450m-lost-cyber-crime-nigeria-senate/ (Date of use: 22 July 2017).

200 Umoru http://www.vanguardngr.com/2017/05/450m-lost-cyber-crime-nigeria-senate/ (Date of use: 22 July 2017).

The Head of the SCC added that the way forward is to develop effective laws, but the Head did not offer proposals on the type of law or amendments that can be categorised as effective.[201] This state of affairs and the response from the SCC suggests that Nigerian consumers will continue to suffer as the government's executive- and legislative arms cannot produce laws that enable it to clump down on cybercrime.

However, Nigeria is not the only country in Africa facing challenges due to its lack of legal infrastructure to safeguard consumers from cybercrime. In South Africa, consumers have been reeling from the spike in cybercrime. Statistics on cybercrime in South Africa indicate that the country has the world's third-largest number of victims.[202]

According to the Banking Risk Information Centre of South Africa (SABRIC), South Africa has the highest rate of cybercrime in Africa. SABRIC and other internet security experts argue that South African consumers are beginning to feel the threat of cyber-attacks.[203] The experts say that many of these attacks come from South African hackers.[204] These attacks have become so severe that consumers in South Africa lose more than US$ 165 million (ZAR 2.2 billion) due to phishing attacks and internet fraud.[205]

Antonio Forzieri, the head of cyber security at Symantec, has underlined the sorry state of cyber security in South Africa and states that in 2014, one in every 214 emails addressed to consumers in the country was a disguised spear-phishing attack.[206] Statistics from the annual Norton Cyber Security Insights Report offer further

---

201 Umoru http://www.vanguardngr.com/2017/05/450m-lost-cyber-crime-nigeria-senate/ (Date of use: 22 July 2017).

202 "SA ranks world's third highest cybercrime victims" 2017 *Business Media Mags* http://businessmediamags.co.za/sa-ranks-worlds-third-highest-cybercrime-victims-2/ (Date of use: 22 July 2017).

203 "SA ranks world's third highest cybercrime victims" 2017 *Business Media Mags* http://businessmediamags.co.za/sa-ranks-worlds-third-highest-cybercrime-victims-2/ (Date of use: 22 July 2017).

204 http://businessmediamags.co.za/sa-ranks-worlds-third-highest-cybercrime-victims-2/ (Date of use: 22 July 2017).

205 http://businessmediamags.co.za/sa-ranks-worlds-third-highest-cybercrime-victims-2/ (Date of use: 22 July 2017).

206 http://businessmediamags.co.za/sa-ranks-worlds-third-highest-cybercrime-victims-2/ (Date of use: 22 July 2017).

confirmation of the deteriorating state of cyber security in South Africa. This Report suggests that more than nine million consumers in South Africa are victims of cybercrimes annually.[207]

According to the Norton Cyber Security Insights Report,[208] researchers surveyed 18,000 consumers from eighteen countries. As a part of the study, they recruited 1,001 online users from South Africa. They used the extrapolation method to multiply the percentage of South African victims by the number of adult online users in South Africa.

This multiplication allows the organisation to estimate the number of online users in the country who are victims of cybercrime over twelve months. The study's results suggest that 8.8 million adult online users in South Africa fall victim to cybercrime annually.

According to the results, *Generation X*-users[209] and *Millennials*[210] shouldered a disproportionate burden of cybercrime. The statistics suggest that 37 per cent of *Generation X*-users and 39 per cent of *Millennials* in South Africa fell victim to cybercrime during the twelve months of the study.[211] The results suggest that the attacks against *Generation X*-users and Millennials were high at a time when statistics showed that South Africans had higher levels of sensitivity to cybercrimes than their counterparts from other developed and developing countries.

The statistics on sensitivity to cybercrime suggest that 76 per cent of South Africans surveyed knew about the spike in the rate of online identity theft, and 67 per cent of the South Africans surveyed knew about the strategies that they could implement to control

---

207 Norton Life Lock "2021 Norton Cyber Safety Insights Report" https://www.nortonlifelock.com/us/en/newsroom/press-kits/2021-norton-cyber-safety-insights-report/ (Date of use: 12 August 2022).

208 Norton Life Lock "2021 Norton Cyber Safety Insights Report" https://www.nortonlifelock.com/us/en/newsroom/press-kits/2021-norton-cyber-safety-insights-report/ (Date of use: 12 August 2022).

209 Refers to the generation born between 1965 and 1978/80 and is currently between 41-56 years old.

210 Refers to the generation born between 1981 and 1994/6 and is currently 25-40 years old.

211 Norton Life Lock "2021 Norton Cyber Safety Insights Report" https://www.nortonlifelock.com/us/en/newsroom/press-kits/2021-norton-cyber-safety-insights-report/ (Date of use: 12 August 2022).

the loss of their personal information over the internet.[212] Despite the high degree of sensitivity towards cybercrime, South Africans were still falling victim to cybercrime. The study suggests that they were falling victim to cybercrime because of their incapacity to take personal responsibility for the security of their personal information in the online environment.

Furthermore, 31 per cent of the *Millennials* surveyed in the study stated that they felt it was more convenient to abandon their online accounts instead of deleting them.[213] The convenience of abandonment suggests that many of these consumers know the steps they need to take to safeguard their online security but are unwilling to do so because they perceive that security measures are inconvenient.

Although the study suggests that South African consumers' failure to take personal responsibility for the security of their personal information in the online world is to blame for the high frequency of cybercrime in South Africa, the reality is that the absence of adequate legal infrastructure is the leading cause of the high prevalence of cybercrime. An analysis of the existing cyber laws suggests that these laws do not go far enough to protect consumers from cybercrimes.

The existing laws merely list the types of crimes committed on the internet and the range of sentences that culprits will face in the event of conviction. Still, they do not punish ISPs or content providers for creating these types of vulnerabilities that increase the susceptibility of South African consumers to cyber-attacks.

Indeed, an analysis of the existing-, and proposed cyber laws also confirms that these laws make no provision for providing security agencies and the courts with authority to issue punitive penalties to content providers and ISPs for the vulnerabilities that render

---

212 Norton Life Lock "2021 Norton Cyber Safety Insights Report" https://www.nortonlifelock.com/us/en/newsroom/press-kits/2021-norton-cyber-safety-insights-report/ (Date of use: 12 August 2022).

213 Norton Life Lock "2021 Norton Cyber Safety Insights Report" https://www.nortonlifelock.com/us/en/newsroom/press-kits/2021-norton-cyber-safety-insights-report/ (Date of use: 12 August 2022).

South African consumers susceptible to cybercrime. These are discussed in chapter three.

An analysis of South Africa's cyber laws suggests that the country has as many as four laws and regulations with provisions that safeguard consumers against security-related risks. Notably, none of these laws contain provisions that hold ISPs and content providers criminally responsible for the conduct that exposes consumers to cybercrime.

The relevant provisions on cybercrime provide security agencies and the courts with the power to arrest and convict the perpetrators of cybercrime. However, they do not give these institutions the authority to arrest and convict ISPs and content providers that aid and abet cyber-criminal activities by designing their services to expose consumers to cybercrime. Some of these laws include:

i. The Independent Communications Authority of South Africa Act 13 of 2000.
ii. The Electronic Communications and Transactions Act 25 of 2002 (ECTA).
iii. The Cryptography Regulations; and
iv. The Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002.
v. The Cybercrimes Act 19 of 2020

Each of these laws purports to protect consumers against cybercrimes. The ECTA has provisions that offer protection to consumers. The ECTA has provisions covering many aspects and categories of cybercrime that might affect consumers. The provisions define the protection afforded to consumers, the punishments imposed against perpetrators of cybercrime (some of which are now repealed), and the duties of various organisations that might monitor the interaction between the consumers and the perpetrators of cybercrime.

However, none of the provisions in the ECTA imposes a responsibility on content providers and ISPs for breaches that leave consumers vulnerable to cyber-criminal attacks.

Indeed, an evaluation of the relevant provisions in the ECTA suggests that it contains provisions that define various categories of cybercrime. The ECTA outlines the types of punishment that the courts may impose against the perpetrators of cybercrime. Still, none of the provisions penalises the ISPs and content providers.

Section 86 of the ECTA outlines the circumstances under which an individual will engage in cybercrime.

Section 86(1) of the ECTA states that a person participates in cybercrime when he intentionally intercepts or accesses electronic data without permission or authority. Section 86(2 provides another definition of cybercrime, stating that a person engages in cybercrime when he interferes with electronic data in a way that destroys it, modifies it, or renders it ineffective.

Section 86(3) adds a third definition of cybercrime when it classifies the unlawful possession, distribution, adoption, procurement, sale, or design of computer programs or electronic devices in a way that influences them to access data or codes to violate any of the provisions of section 86, as a cybercrime.

Further, section 86(4) states that a person engages in cybercrime when he uses the program or device mentioned in section 86(3) to circumvent cyber security measures that consumers and other organisations have implemented to prevent intruders from accessing data.

Section 87 of the ECTA outlines the definitions of computer-related forgery, fraud, and extortion.

Section 87(1) states that a person commits the crime of extortion, fraud, and forgery when he threatens to engage in any of the cybercrimes defined in section 86 of the ECTA to obtain a proprietary advantage through unlawful means.

Section 87(2) of the same law states that a person commits the crimes of forgery, extortion, or fraud when he utilises any of the crimes outlined under section 86 of the

ECTA to cause the generation of fake data that leads other people or institutions to act on it because they believe that it is genuine data.

The brief review of the individual provisions above confirms that they only define various categories of cybercrime and impose hefty punishments on the perpetrators. The provisions suggest that the government has attempted to respond to the high rates of cybercrime by enacting laws that protect consumers if they lose their personal information or money to cyber-criminals.

Whereas many of the outlined provisions purport to safeguard consumers from cybercrime, none of them gives security agencies and the courts the authority to charge and convict ISPs and content providers who increase the vulnerability of consumers to cybercrimes. The highlighted provisions state that individuals responsible for cybercrimes are the ones who are directly responsible for the criminality.

The legislature's decision to incorporate the term "intentionally" in the laws suggests that the legislator did not want to hold content providers and ISPs criminally responsible for the conduct that exposes consumers to the adverse outcomes of, *inter alia*, internet fraud and identity theft. It suggests that the legislature aims to prosecute individuals and organisations that engage in cybercrime. However, it allows ISPs and content providers to continue expanding without worrying about their obligations towards consumers who use their services.

In the current digital climate, ISPs and content providers are expanding quickly and, in turn, their customer base is growing. This expansion is increasing the number of consumers and organisations exposed to cybercrime. The high prevalence of cybercrime in South Africa illustrates consumers' increased exposure to cybercrime.

Despite widespread evidence indicating that the number of South Africans exposed to cybercrime is increasing, the ECTA has not imposed obligations that compel content providers and ISPs to implement security measures to safeguard consumers. Therefore,

the absence of provisions in the ECTA that compel service providers to protect consumers has left many without adequate protection against cyber-criminals.

2.4.2 LEGAL INFRASTRUCTURE INEFFECTIVENESS IN PROTECTING THE GOVERNMENT

In addition to the weaknesses in protecting consumers, the weak legal infrastructure is ineffective in safeguarding the interests of the State. The existing legal regime does not offer the type of protection needed to prevent ISPs and content providers from infringing on the interests of the State.

Specifically, the legal regime does not give the country and State agencies the power to penalise ISPs and content providers who undermine the interests of the State by exposing it to vulnerability, which may question its legitimacy. The ECTA and the Cryptography Regulations[214] are the applicable laws concerning the protection of the interests of the State in South Africa. As the enabling law, the ECTA outlines the key definitions and powers of the government concerning organisations that specialise in the provision of cryptography services.

The Cryptography Regulations outline the rules regarding the registration of cryptography providers. The Regulations state the type of information that cryptography service providers must disclose to the Director General (DG) in their registration.

Key provisions in the ECTA and the Cryptography Regulations define the extent of the powers of government regarding the regulation of service providers. Still, they do not go far enough to safeguard the State from the conduct that might undermine its legitimacy and contribute to its collapse.

An analysis of the critical provisions confirms that they do not give the government the necessary powers it requires to safeguard its interests.

---

[214] ECTA Cryptography Regulations No. 8418 of 10 March 2006.

Section 1 of the ECTA defines three critical terms for appreciating the government's and ISPs' relationship. These terms are "*cryptography service*," "*cryptography provider*," and "*cryptography product*." The section defines cryptography service by covering all categories of services in which a company uses cryptographic techniques to ensure that the recipient of data messages, or individuals storing data messages, can limit the number of persons and organisations that can access or read the message by controlling its intelligibility.

It also defines "*cryptography services*" as using cryptography techniques to guarantee the data's authenticity, integrity, and source. Section 1 of ECTA defines cryptography products as:

> [A]ny computer software or hardware that aids the recipient or the sender of data messages to use cryptography techniques to safeguard the data by controlling its intelligibility, authenticity, integrity, or source.

Section 1 of the ECTA states that "*cryptography provider*" is a phrase that denotes all persons or organisations that offer cryptography services in South Africa. This section outlines the definition of terms related to cryptography. Still, it does not provide the government the power that would allow it to prevent people from using cryptography services to threaten its interests.

In addition to section 1, the Chapter on cryptography providers offers further guidelines on the law relating to regulating companies that specialise in cryptography services. Still, they do not provide the types of powers that South African security agencies require to prevent cryptography providers from engaging in activities that might undermine the legitimacy of the State.

The Chapter on cryptography providers covers sections 29, 30, 31, and 32 of the ECTA. The Chapter outlines the regulations that pertain to cryptography providers.

Section 29 of the ECTA gives the DG the authority to maintain a Register of all companies specialising in providing South Africa's cryptography services.

Section 29(2) of the ECTA states that the Register of those companies must include their name, address, cryptography services delivered, and other important information essential for locating the company.

Section 29(3) of the ECTA bars the DG from compelling service providers to disclose information they consider confidential or any other type of information they would regard as part of their trade secrets.

Section 30 of the ECTA bars companies from delivering cryptography services within the country before they have complied with the registration requirements under section 29. Section 30 of the ECTA provides the three conditions under which the ECTA will regard a service provider as delivering its services within South Africa.

Section 30(3)(a) of the ECTA states that a company will provide cryptography services within South Africa if it delivers them from premises within the country. Section 30(3)(b) of the ECTA states that a person or organisation will provide cryptography services within South Africa if it delivers its services to an individual in the country when he utilizes the cryptography services.

Section 30(3)(c) of the ECTA states that a person or organisation will be delivering cryptography services within South Africa if it delivers the services to an individual or organisation that uses it for a business that operates in South Africa. The essence of section 30 is that it outlines the scope of the application of the provisions on cryptography.

It suggests that the law covers South African companies and companies registered in other parts of the world but offers cryptography services to consumers and organisations in South Africa. Section 31 of the ECTA bars the DG from giving unauthorised access to information contained in the register of service providers.

However, section 31(2) of the ECTA outlines the exceptions to the rule on the DG's authority to disclose information to third parties. Section 31(2) of the ECTA states that the bar does not apply in five situations.

First, the bar against disclosure does not apply to instances where an authorised agency investigates a criminal offence. Second, the prohibition against disclosure does not apply when government agencies tasked with providing peace and security are the source of the request for information. Third, the bar against disclosure does not apply when the cyber inspector requests that information. Fourth, the bar does not apply to instances where a person or organisation makes a request under sections 11 and/or section 30 of the PAIA.[215] Finally, the bar does not apply to instances where the request for information is pursuant to civil proceedings relating to the provision of cryptography services.

Section 32(1) of the ECTA also exempts the State Security Agency or SSA (formerly known as the National Intelligence Agency) from the bar against access to information and any other provision of the Chapter on cryptography providers. Section 32(2) of the ECTA states that all individuals or organisations contravening the provisions of the Chapter on Cryptography will be eligible for a fine or a two-year prison term.

Some exceptions under section 31(2) and section 32(2) of the ECTA suggest that the government has the necessary powers to investigate and prevent ISPs and content providers from engaging in activities that might undermine its interests. The exceptions that give the government such powers are the exceptions related to the security and safety of the country, the exception on investigations of criminal offences, and the exception on the SSA.

The exception on security and safety of the country suggests that the government can make an official request for information from the DG and the cryptography providers if it believes that such data is essential for the security and safety of the country. Where the government believes that the information the cryptography providers are relaying is a threat to the country's national security, it can make an official application to the DG or the cryptography providers.

[215] Promotion of Access to Information Act 2 of 2000 (hereinafter referred to as "PAIA").

The exception on criminal proceedings suggests that the courts can order the DG to provide information on the services that cryptography providers deliver to their clients if such information is crucial to resolving a crime.

This would be the case where investigative agencies believe that the perpetrator of a crime used the cryptography product to relay incriminating information from one user to another. In such an instance, the court can compel the cryptography providers and the DG to supply that information for the speedy resolution of the crime.

The exception on the SSA suggests that the Chapter on cryptography providers does not apply to it.

It suggests that the SSA has the power to access information on the services of companies that specialise in the provision of cryptography services. The SSA has no limitation on the type of information it can access. Therefore, it can access cryptography providers' codes to encrypt information consumers share regularly. Accessing the codes means the SSA can spy on consumers and identify individuals with ulterior motives.

While it is true that the listed exceptions give the government room to look into the activities of companies that provide cryptography services, none of the exceptions goes far enough to give the government the types of powers that would lead it to control these companies and prevent them from engaging in activities that will undermine its interests.

The exceptions merely state the circumstances where security agencies and courts will access information on the activities of the service providers. In fact, sections 29(3) and 32(2) of the ECTA further curtail those powers by placing restrictions on the nature of the information that cryptography providers can disclose to service providers and the scope of punishment such companies will face if they fail to comply with the rules outlined in the Chapter on cryptography providers. Section 29(3) limits the scope of information provided to the DG to information that does not disclose the cryptography providers' trade secrets and confidential information.

This restriction means that the government cannot compel cryptography providers to share the types of information that will lead them to gain access to the encryption codes. It means that the government cannot force cryptography providers to give them a back door into the software and hardware they use to encrypt data that people and organisations in South Africa are sending and receiving.

Such a backdoor would make it easier for the South African government to monitor communications and ensure that people are not sending information that might undermine its legitimacy. Section 32(2) limits the scope of the responsibility of service providers, stating that individuals and companies that violate the provisions of the chapter on cryptography providers will be eligible for a fine and/or a two-year prison term.

Such a lenient sentence places the power in the hands of cryptography providers by giving them room to reject the requests for information by security agencies in South Africa. The lenient sentencing guidelines also suggest companies can take risks and implement processes that challenge the government's interests. The companies will realise that the risk of violating the Chapter is minimal. Therefore, they will not think twice when processing the data of individuals who want to subvert the country’s system of government and the governance structures that are essential to the legitimacy of the State.

These limitations make it difficult for the government to safeguard its interests by using the national security exception under section 31 to compel cryptography providers to furnish it with the information that will make it easier for it to monitor the real-time communications of individuals that are a threat to the country’s safety and security. The limitations imply that the government’s powers are inadequate for it to hold foreign- and local cryptography providers responsible whenever their activities, products, or services undermine the interests of the State.

Indeed, the government will face further restrictions from constitutional provisions safeguarding the right to privacy and freedom of expression. The government’s attempt

to use the ECTA as the basis for accessing information from cryptography providers will fail if a person challenges it because exercising power violates constitutional provisions protecting the right to privacy and freedom of expression.

Section 16 of the Constitution[216] enshrines the freedom of expression. This section states that all South African people can freely express themselves. This right includes the freedom to receive and disseminate ideas and information and the right to have a free press.

Section 14 of the Constitution enshrines the right to privacy. The section states that all South Africans have the right to privacy and adds that the right bars the state from infringing on the privacy of their communication. Section 7 of the Constitution states that the Bill of Rights is one of the cornerstones of the country's democracy. Section 8 states that the Bill of Rights applies to the judiciary, the executive, the legislature, and all other organs of the State in the country.

The absence of an express provision in the ECTA providing the government with the power to hold cryptography providers accountable for the actions of their customers means that the security agencies cannot survive constitutional challenges related to privacy and freedom of expression.

In addition, the absence of provisions which compel cryptography service providers to provide information to security agencies in the interest of protecting state interest, makes it easier for cryptography providers to challenge the constitutionality of the government's request for information.

The companies can launch constitutional petitions that seek to determine whether the request for information constitutes a violation of the customer's privacy rights. They can also argue that the request for information violates section 29(3) of the ECTA, which

[216] Constitution of the Republic of South Africa, 1996 (hereinafter referred to as the Constitution).

bars the government from requesting information that companies categorise as trade secret or confidential.

The company can argue that providing such information to the South African government will be detrimental to its long-term interests because it will lose customers, making it easier for competitors to imitate their services. The company can also assert that releasing proprietary information will be detrimental to their interests because it would make their cryptography services vulnerable to attacks by cyber-criminals.

Although the South African government has not experienced the challenges that might arise from the weak legal regime, evidence from the experience of other States in Africa and Asia offers some crucial insight into the nature of the threat that the State faces.

African and Asian States that fell victim to the Arab Spring revolts can illustrate the national security challenges arising from the failure to regulate ISPs and content providers.[217] The Arab Spring revolutions in Egypt, Tunisia, and Libya have already demonstrated some dangers that might arise from the unregulated interaction between online users, content providers, and ISPs. During that revolution, protesters relied on social media networks like WhatsApp, Twitter, Facebook, and YouTube. They used mobile devices, such as iPhones and Blackberries, to organise the protests and share information targeted at toppling the Hosni Mubarak administration.[218]

They relied on social media services and smartphone devices because of their awareness that the safeguards installed on Facebook, Twitter, WhatsApp, and YouTube prevent third parties from knowing the source of the information they are sending and receiving.[219] Furthermore, the organisers of the protests used the WhatsApp platform

---

217 Beaumont "The truth about Twitter, Facebook and the uprisings in the Arab world" *The Guardian* 2011 https://www.theguardian.com/world/2011/feb/25/twitter-facebook-uprisings arab-libya (Date of use: 22 July 2017).

218 Hempel "Social media made the Arab Spring, but couldn't save it" *Wired* 2017 https://www.wired.com/2016/01/social-media-made-the-arab-spring-but-couldnt-save-it/ (Date of use: 22 July 2017).

219 Eltantawy & Wiest 2011: 1207.

because of its end-to-end encryption, which prevented the government from monitoring the information they were sending and receiving.[220]

They would establish WhatsApp groups and use them to organise the protests. The government's attempts to prevent the organisers of the demonstrations from using social networking sites failed because the country lacked an effective legislative framework for regulating the interaction between internet users, ISPs, and content providers.[221] The government lacked the legislative mandate to prevent companies like WhatsApp, Apple, and Blackberry from delivering their cryptography services to protesters wishing to overthrow the State.

Protesters and rioters continued to use social media technologies to share information that was damaging to the national security of Egypt, Libya, and Tunisia, even after their respective governments announced that they were conducting a crackdown on those technologies. The outcome was the ousting of the Egyptian government, the Libyan government, and the Tunisian government following the emergence of the weak administrations and insurgent groups that posed a threat to the well-being of the State and citizens in these countries.

Like Egypt, Libya, and Tunisia, the Chinese government faced similar challenges during the pro-democracy protests in 2014 in Hong Kong. Organisers of those protests used cryptography products and services to prevent security services from knowing their identity and intercepting their communications. They would use platforms like WhatsApp to discuss the extra-legal measures they would use to force the Chinese government to accept their pro-democracy demands. They would use the platforms to organise the strategy to seize government buildings and roads.

220 Eltantawy & Wiest 2011:1207.
221 Eltantawy & Wiest 2011: 1208.

The platforms made it easier for them to carry out their operations in a way that did not give out the identities of the individuals and organisations leading the protest.[222] Alex Yeung, one of the participants in the protests, confirmed this when he informed the New York Times that WhatsApp played an instrumental role in the success of the protests.[223] He claimed that WhatsApp made it easier for protesters to stay one step ahead of authorities by identifying protest zones and coordinating the personnel demands at their first-aid tents.[224]

He added that other platforms like Google and Facebook were integral to their quest to disseminate information.[225] Organisers of the protest used Google Documents and Facebook Pages to list items needed to make the protests successful. They would order umbrellas, facemasks, packaged snacks, and bottled water using these platforms.[226]

Cryptography providers such as WhatsApp, Facebook, Apple, Blackberry, and Twitter were instrumental in enabling protesters to send and receive information on the protests using processes and systems inaccessible to Chinese security agencies.[227]

The companies made it easier for protesters to exchange information on protest zones, supplies, and other essential issues to sustain their protests against the Chinese government.[228] The protesters' success in evading the Chinese security agencies led the Chinese government to block people in Hong Kong from accessing WhatsApp

---

222 Buckley & Ramzy "Hong Kong protests are leaderless but orderly" 2014 *The New York Times* https://www.nytimes.com/2014/10/01/world/asia/in-hong-kong-clean-and-polite-but-a protest-nonetheless.html (Date of use: 22 July 2017).

223 Buckley & Ramzy https://www.nytimes.com/2014/10/01/world/asia/in-hong-kong-clean-and polite-but-a-protest-nonetheless.html (Date of use: 22 July 2017).

224 Buckley & Ramzy https://www.nytimes.com/2014/10/01/world/asia/in-hong-kong-clean-and polite-but-a-protest-nonetheless.html (Date of use: 22 July 2017).

225 Buckley & Ramzy https://www.nytimes.com/2014/10/01/world/asia/in-hong-kong-clean-and polite-but-a-protest-nonetheless.html (Date of use: 22 July 2017).

226 Buckley & Ramzy https://www.nytimes.com/2014/10/01/world/asia/in-hong-kong-clean-andpolite-but-a-protest-nonetheless.html (Date of use: 22 July 2017).

227 Chen et al. "Apps speed up, and often muddle, Hong Kong protesters' messages" 2014 *The Wall Street Journal* https://www.wsj.com/articles/whatsapp-key-to quickly-rallying-protesters-in-hong-kong-but-groups-struggle-to-stay-on-message 1412878808 (Date of use: 22 July 2017).

228 Chen et al.https://www.wsj.com/articles/whatsapp-key-to-quickly-rallying protesters-in-hong-kong-but-groups-struggle-to-stay-on-message-1412878808 (Date of use: 22 July 2017).

cryptography services. The Chinese government tightened its control over ISPs and content providers by instituting a partial block on the WhatsApp platform.

The Chinese government used the *Great Firewall System* to block WhatsApp and other companies like Google, Telegram, and Facebook from providing cryptography services to internet users and business entities in China.[229] In addition to restricting WhatsApp, Telegram, Google, and Facebook, the Chinese government imposed restrictions on Virtual Private Networks (VPNs) and other websites that assist in live-streaming videos.[230] The Chinese government excluded WeChat from the list of blocked companies because it agreed to give the government a backdoor, making it easier for security agencies to monitor encrypted messages, videos, and data subscribers shared on the site. WeChat has more than 900 million subscribers. This permission meant that the Chinese government could access the services of the cryptography provider to assess whether the information subscribers were sharing was undermining the interests of the State.[231] The ban on WhatsApp meant that the Chinese government had shut down one of the few cryptography service providers that gave internet users access to a free and encrypted messaging service.

The Chinese government's attempts to block foreign- and local cryptography providers that were not complying with existing laws have been successful because it had the legal authority and technological resources necessary to implement such policies. Unlike the governments in Egypt, Libya, and Tunisia, the Chinese government had the legal- and technological infrastructure needed to hold cryptography providers responsible for the actions of their customers, which undermined the interests of the State.

---

229 Haas "China blocks WhatsApp services as censors tighten grip on internet" 2017 *The Guardian* https://www.theguardian.com/technology/2017/jul/19/china-blocks-whatsapp services-as-censors-tighten-grip-on-internet (Date of use: 22 July 2017).

230 Haas "China blocks WhatsApp services as censors tighten grip on internet" 2017 https://www.theguardian.com/technology/2017/jul/19/china-blocks-whatsapp-services as-censors-tighten-grip-on-internet (Date of use: 22 July 2017

231 Haas "China blocks WhatsApp services as censors tighten grip on internet" 2017 https://www.theguardian.com/technology/2017/jul/19/china-blocks-whatsapp-services as-censors-tighten-grip-on-internet (Date of use: 22 July 2017).

Like Egypt, many other African states, and other parts of the world, the South African government lacks the legal framework to regulate interactions between content providers, internet users, and ISPs. The existing legal infrastructure does not give the South African government adequate powers in issues related to the regulation of cryptography providers.

The existing laws give cryptography providers the power to reject requests to disclose information that they consider proprietary. It gives them the power to challenge the requests for information whenever they believe such requests violate the privacy rights of the country's citizens and the right of citizens to express themselves freely. Weak cyber laws might undermine national security by creating avenues for criminal gangs and other individuals with dubious intent, granting them the power to topple the government. Weaknesses in the existing legal framework make it impossible for the State and security agencies in South Africa to take the measures the Chinese government instituted against cryptography providers.

The Chinese government blocked cryptography providers that were reluctant to comply with the country's laws and were aiding and abetting the activities of groups that wanted to overthrow the rule of the Chinese government in Hong Kong. Egypt and other Asian and African countries affected by the Arab Spring revolution failed on this front because they lacked the legal- and technological infrastructures needed to punish cryptography providers, undermining the interests of the State.

The South African State is vulnerable to the activities of cryptography providers because the country lacks the legal- and technological infrastructure needed to regulate the activities of local- and international companies that provide cryptography services in South Africa. The existing laws merely require companies to provide information that would make it easier for the government to know their address and the services they deliver to consumers and organisations in South Africa.

However, the laws do not give the government the power to ban or impose partial blocks on providers of cryptography services that are intent on compromising the interests of

the State. The success of the Arab Spring revolts, the difficulties the Chinese government faced in controlling pro-democracy protests, and the weak legal framework in South Africa all form the basis for analysing the laws regulating internet use in South Africa.

Ascertaining an overall appraisal of the laws and regulations dedicated to ISPs creates an opportunity to determine the possibilities of South African internet access in terms of local competition in the global expansion of ISPs and services. This allows for a comparison between Nigerian-, Egyptian-, and South African ISPs and internet users to ascertain the impact of internet use on a country's overall ability to sustain itself in the marketplace based on compliance with national laws. It also permits an analysis of the effectiveness of existing laws in safeguarding the interests of the State at a time when cryptography providers have the power to conduct their activities in a way that might undermine those interests.

Additionally, it permits an investigation into national laws' role in preventing cryptography providers from engaging in actions that have threatened the States of Egypt, Tunisia, China, Libya, Syria, and Bahrain. This creates room for an analysis of the constitutionality of cryptography laws, considering the constitutionally protected right to privacy and freedom of expression. The latter is, however, not the focus of this research.

An investigation into South Africa's cryptography laws will pave the way for a compelling analysis of the measures South Africa can take to safeguard its interests. This analysis assesses whether the existing law creates adequate room for the government to safeguard its interests.

2.5 PRELIMINARY CONCLUSION

In this chapter, the researcher provided an overview of ISPs in terms of their historical development, current place in the international arena and the challenges posed by and to ISPs when considered against rising cybercrime and a world where revolution and revolt – often aided and abetted by the internet - take a central place in politics. The

researcher provided an overview of the current weaknesses and challenges posed by the South African national law concerning ISPs and end-users with nefarious intent and demonstrated that weaknesses are inherent in the current South African law when measured against China and Nigeria. In the next chapter, the researcher considers the role and liability of ISPs within the domestic context of South African law to extrapolate further the challenges discussed synoptically above.

CHAPTER THREE

THE ROLE AND LIABILITY OF INTERNET SERVICE PROVIDERS IN SOUTH AFRICA

3.1 INTRODUCTION

In this chapter, the researcher contextualises the research and discusses the role and liability of ISPs in South Africa, cognisant of the perspectives provided in chapters one and two. The chapter opens with a historical view from the South African context and then moves to contemporary challenges and current legal responses. The research proceeds cognisant that South African internet laws operate within the global community to protect citizens. It is trite that each jurisdiction's legislative authority decides how much or little control may be instituted over telecommunication. *Prima facie*, the South African legislature, has extended limited powers concerning the degree of control over the internet and telecommunication. This chapter contextualises the South African situation for later comparison with China, Ireland, and Nigeria.

This chapter presents a critique over and above the points already addressed in Chapters One and Two. The researcher contextualizes the role and liability of ISPs through the lens of the Constitution of the Republic of South Africa, 1996, the Protection of Personal Information Act, No. 4 of 2013 (POPI Act), the Electronic Communications and Transactions Act, No. 25 of 2002 (ECT Act), and other relevant legislation. These legal frameworks form the foundation for understanding the regulatory environment within which ISPs operate in South Africa and define their responsibilities and liabilities in various contexts.

The chapter acknowledges the interplay between South African internet laws and the broader global digital community. It highlights the country's efforts to align with international standards in protecting its citizens in the digital realm. A critical examination of South Africa's legislative approach to telecommunications and the internet is

undertaken, examining the extent and limitations of governmental control and oversight in these sectors.

Central to this chapter is the exploration of the nuanced powers vested in the South African legislature regarding the regulation of the Internet and telecommunications. The chapter evaluates the balance struck by South African law between regulation, control, and the promotion of digital freedoms and rights. This includes an analysis of the current legal mechanisms in place, their effectiveness, and the challenges they face in addressing issues such as cybercrime, data protection, and ISP liability.[232]

This chapter lays the groundwork for subsequent comparative analysis of the legal frameworks and ISP regulatory environments in China, Ireland, and Nigeria by contextualising the South African situation. This comparative dimension aims to provide a broader understanding of how different jurisdictions navigate the complex landscape of Internet governance and the responsibilities and liabilities of ISPs within varying legal and socio-economic contexts.

3.2 INTERNET SERVICE PROVIDERS – HISTORICAL DEVELOPMENT

In this section, the researcher contextualizes the South African ISPs and their historical development, tracing the journey from the pre-constitutional era through to the post-constitutional period, culminating in the most recent amendment under the Electronic Communications and Transactions Amendment Act, No. 1 of 2014 (ECT Amendment Act). The overall purpose of this discussion is to narrate the evolution of ISPs in South Africa, highlighting the significant transformations brought about by the constitutional dispensation and subsequent legal reforms.

The historical development of ISPs in South Africa can be segmented into distinct phases. With limited private-sector involvement, the telecommunication landscape was

[232] Dharmawan et al. 2019: 3175.

primarily state-controlled during the pre-constitutional era. The advent of the democratic era brought about significant policy shifts marked by liberalization and deregulation in the telecommunications sector. This period saw the entry of private ISPs into the market, fostering competition and innovation.[233]

Legislative reforms further accelerated post-constitutional developments to align the telecommunication sector with the new constitutional values of openness and access to information. Key among these reforms was the enactment of the Electronic Communications and Transactions Act, No. 25 of 2002, which provided a regulatory framework for electronic communications and transactions, including provisions specific to ISPs.[234] The ECT Amendment Act 1 of 2014 further refined the regulatory environment, addressing contemporary challenges such as cybersecurity, data protection, and consumer rights.[235] This amendment signifies the ongoing commitment of the South African legislature to adapt and respond to the dynamic nature of digital communications and the role of ISPs.

Throughout this historical journey, various case law and academic articles have shed light on the evolving roles and responsibilities of ISPs. Critical judicial decisions have interpreted the legal provisions pertaining to ISPs, influencing their operational practices, and shaping the regulatory landscape. Academic discourse has critically analyzed these developments, offering insights into the effectiveness, challenges, and prospects of ISP regulation in South Africa. The historical development of ISPs in South Africa is a narrative of transition from a state-controlled to a more liberalized sector, underscored by legal reforms that reflect the country's constitutional values and the imperatives of a digital age.[236]

233 Dharmawan et al. 2019: 3175.
234 Dharmawan et al. 2019: 3175.
235 Eltantawy & Wiest 2011: 1209.
236 Eltantawy & Wiest 2011: 1209.

3.2.1 PRE-CONSTITUTIONAL ERA

In the era preceding South Africa's constitutional democracy, the development of ISPs and the broader telecommunications landscape significantly differed from the post-constitutional era. This period, marked by apartheid policies and state control, set a unique backdrop for the evolution of digital communications and ISP services in the country.

During the pre-constitutional era, South Africa's telecommunications sector was heavily dominated by state control. Through entities like Telkom, the government had a monopoly over telecommunication services. This monopolistic approach reflected the country's broader political and economic landscape, where state control was pervasive in critical sectors. The lack of competition in the telecommunications industry meant innovation was stifled, and the growth of services, including internet provision, was significantly slower than global trends.

The inception of internet services in South Africa can be traced back to this period, albeit in a very nascent form.[237] The initial connections to the global internet were established mainly through academic and research institutions. These connections were rudimentary and limited in scope, primarily used for academic and research purposes.[238] The commercialization of Internet services was still a distant concept, and the public had minimal access to these early forms of the Internet.

The regulatory framework governing telecommunications during the pre-constitutional period was characterized by strict government regulations and policies favouring state monopolies. There was little legislation specifically targeting ISPs or internet regulation, as the internet was still in its infancy and not widely recognized as a significant communication medium.[239] The regulatory environment, therefore, did not encourage

237 Nyinevi & Ayalwe 2022: 101.
238 Nyinevi & Ayalwe 2022: 101.
239 Nyinevi & Ayalwe 2022: 101.

the entry of private players into the market, further entrenching the state's dominance in telecommunications.

Despite the isolation experienced by South Africa during the apartheid years, the country was not entirely cut off from global technological advancements. International developments in telecommunications and information technology did have some limited influence on the South African context.[240] These influences began to sow the seeds for future changes in the ISP landscape, although the full impact of these developments would only be realized in the post-apartheid era.

The socio-political environment of South Africa during this period also played a significant role in shaping the telecommunications sector. The apartheid regime's policies of segregation and control extended to ICTs. Access to technology and information was highly regulated, and the digital divide reflected the broader societal inequalities.[241] This context significantly influenced how telecommunications services, including internet access, were developed and deployed.

3.2.2 POST-CONSTITUTIONAL ERA

The advent of South Africa's constitutional democracy marked a significant turning point in the development of ISPs and the telecommunications sector. This post-constitutional era is characterized by liberalization, regulatory reforms, and an increased recognition of the importance of digital technology in the country's socio-economic development.

One of the most pivotal changes in the post-constitutional era was the liberalization of the telecommunications sector. The government moved away from the apartheid-era policies of state control, opening the market to competition.[242] This shift was critical in stimulating growth and innovation within the ISP industry. Private companies and new entrants could now offer internet services, leading to increased competition, improved

240 Nyinevi & Ayalwe 2022: 101.
241 Eltantawy & Wiest 2011: 1209.
242 Eltantawy & Wiest 2011: 1209.

service quality, and reduced consumer prices.[243] This period saw a significant increase in internet accessibility and usage nationwide.

Accompanying the liberalization of the market were comprehensive regulatory reforms aimed at creating an environment conducive to fair competition and consumer protection.[244] The Telecommunications Act of 1996 and its subsequent amendments played a crucial role in shaping the regulatory landscape for ISPs. These legislative measures were designed to break down monopolies, establish independent regulatory bodies, and set standards for fair practices and service quality.

Another significant piece of legislation was the Electronic Communications Act of 2005, which further refined the legal framework for electronic communications, including Internet services. This Act addressed various aspects of telecommunications, from service provider licensing to managing the radio frequency spectrum and consumer rights.[245]

The post-constitutional era witnessed substantial growth in the ISP industry. The number of service providers increased, and there was a notable expansion in the range and quality of internet services available to South Africans.[246] Broadband internet became more widely accessible, and mobile internet saw exponential growth, driven by the widespread adoption of smartphones.

However, this growth was not without challenges. The digital divide remained a significant issue, with disparities in internet access between urban and rural areas and among different socio-economic groups. Additionally, ISPs faced challenges related to infrastructure development, particularly in underserved areas, and in adapting to the rapidly changing technological landscape.[247]

---

243 Zarei et al. 2019: 198.
244 Eltantawy & Wiest 2011: 1209.
245 Eltantawy & Wiest 2011: 1209.
246 Reddick et al. 2020: 102904.
247 ISS Africa, "South Africa Lays Down the Law on Cybercrime," https://www.issafrica.org (Date of use 9 January 2024).

As internet usage grew, so did concerns over cybersecurity and data protection. The government and regulatory bodies emphasised safeguarding digital data and protecting users from cyber threats. Legislation, such as POPIA, was introduced to regulate the processing of personal information and protect individuals' privacy.[248]

With the growth of the internet and related technologies, ISPs found themselves at the centre of various legal and ethical debates. Issues around ISP liability, content regulation, and freedom of expression became increasingly prominent. ISPs were required to navigate complex legal requirements while balancing the needs and rights of their users.

3.3 CONTEMPORARY THEMES

The contemporary structure for regulating ISPs gives rise to certain contentious concepts and themes – some extrinsic and some intrinsic - which are central to this research. These are discussed below before the researcher moves to problematise the role and liability of ISPs against these factors.

3.3.1 INTERNATIONAL OBLIGATIONS

International obligations and standards significantly influence the global landscape of Internet governance and the role of ISPs. For South Africa, aligning with these international norms is a matter of legal compliance and a strategic alignment with global best practices in the digital domain.[249]

Various treaties, agreements, and cooperative frameworks shape how nations, including South Africa, manage and regulate ISPs in international obligations. One of the cornerstones of international agreements in this context is the ITU Regulations. The ITU, a specialized agency of the UN, provides guidelines and standards for telecommunications, including internet services.[250] As a member state, South Africa

248 Zarei et al. 2019: 198.
249 Major 2021: 44.
250 Flyverbom et al. 2019: 4.

must align its policies and regulatory frameworks with ITU standards, which cover a range of aspects from spectrum allocation to cybersecurity measures.

Another critical international framework is the World Trade Organisation's (WTO) General Agreement on Trade in Services (GATS), which includes commitments to telecommunications services. These commitments influence how South Africa opens its telecommunications market to foreign service providers and investment, impacting the competitive landscape for ISPs within the country.[251]

Apart from these broad frameworks, specific international conventions address issues directly impacting ISPs. For instance, the Budapest Convention on Cybercrime is an essential international treaty that outlines cooperative measures for combating cybercrime. Although South Africa is not a signatory to this convention, its principles and guidelines influence global norms and practices, which South Africa considers in its cybersecurity and ISP regulatory strategies.[252]

The role of ISPs in data protection and privacy is also subject to international standards, influenced by the European Union's General Data Protection Regulation (GDPR). While GDPR is a regional regulation, its extraterritorial implications affect how global ISPs, including those operating in South Africa, handle personal data.[253] Compliance with international data protection standards is crucial for ISPs, especially those with transnational operations or handling data from jurisdictions where these rules apply.

On the African continent, the African Union's Convention on Cyber Security and Personal Data Protection, also known as the Malabo Convention, sets out to harmonize cybersecurity and data protection laws across Africa. South Africa's approach to ISP regulation is influenced by such regional commitments, aiming to ensure consistency and cooperation in digital policies across the continent.[254]

---

251 Zarei et al. 2019: 198.
252 Major 2021: 44.
253 Major 2021: 44.
254 Flyverbom et al. 2019: 4.

Engagement with international bodies like the Internet Governance Forum (IGF) and the World Summit on the Information Society (WSIS) also shape South Africa's stance on ISP-related issues.[255] These platforms provide opportunities for dialogues on public policy issues related to Internet governance, allowing South Africa to align its domestic policies with emerging global trends and challenges.

However, navigating these international obligations is not without challenges. Balancing national interests with global commitments, especially in areas like internet censorship, surveillance, and the free flow of information, can be complex. South Africa struggles with adhering to international norms and protecting its national security and cultural values.

The commitment to international obligations also extends to digital divide issues and internet accessibility. As part of the global community, South Africa is conscious of the United Nations' Sustainable Development Goals (SDGs), particularly Goal 9, which emphasizes the role of infrastructure and innovation, including ICT, in development.[256] This aligns with South Africa's objectives to enhance ISP services for broader and more equitable internet access.

In the sphere of trade and commerce, South Africa's commitments under various bilateral and multilateral trade agreements have implications for ISPs, especially concerning cross-border data flows and e-commerce regulations.[257] These agreements often include electronic communications and digital services provisions, impacting how ISPs operate within the global market.

Thus, international obligations are pivotal in shaping the legal and regulatory environment for ISPs in South Africa. By aligning with these international norms, South Africa ensures compliance with global standards and positions its ISP industry to be competitive and responsive to the evolving global digital landscape. This commitment to

255 Flyverbom et al. 2019: 4.
256 Lembani et al. 2020: 77.
257 Flyverbom et al. 2019: 4.

international obligations reflects a strategic approach to fostering a robust, secure, and inclusive digital environment within the country.

3.3.2 CONSTITUTIONAL FRAMEWORK

The constitutional framework of South Africa plays a critical role in shaping the regulatory environment for ISPs and forms the bedrock of their operational and legal context. The Constitution underpins the nation's legal system and sets out the fundamental principles and rights that govern the interaction between the state, ISPs, and the citizens.

The Bill of Rights is particularly significant for ISPs. It guarantees rights directly relevant to digital communication and internet services. Key among these rights is the right to privacy (section 14), which impacts how ISPs handle personal data and user information. In the age of digital communication, protecting personal information is paramount, and ISPs are at the forefront of ensuring compliance with this constitutional mandate.[258] This right to privacy also intersects with issues around surveillance and data retention by ISPs, which have become increasingly pertinent in recent years.

Freedom of expression is another constitutional right directly impacting ISPs (section 16). This right includes the freedom to receive or impart information or ideas, a cornerstone of Internet communication. ISPs, therefore, play a critical role in facilitating this right, even as they navigate the complex terrain of content regulation, censorship, and the removal of unlawful content.[259] Balancing the freedom of expression with other competing rights and societal interests, such as national security and public morality, remains a challenging yet essential duty for ISPs operating within South Africa's constitutional framework.

The constitutional principle of equality and non-discrimination (section 9) also has implications for ISP operations. ISPs have a role in ensuring that internet services are accessible to all without discrimination on any grounds. This principle is particularly

[258] Lembani et al. 2020: 77.
[259] Flyverbom et al. 2019: 7.

relevant in addressing the digital divide in South Africa and ensuring equitable access to digital resources and services.

Moreover, the Constitution mandates the right to access information (section 32), which underscores the role of ISPs in providing open and transparent access to information.[260] This right is foundational to the concept of an informed citizenry and a transparent, accountable government, making ISPs crucial facilitators in realizing this constitutional promise.

The Constitution also provides for administrative justice (section 33), which requires lawfulness, reasonableness, and procedural fairness in administrative actions. This impacts how regulatory bodies overseeing ISPs operate and make decisions affecting the industry, ensuring that ISPs are regulated in a manner that is consistent with these constitutional principles.

In the broader context, the constitutional framework shapes the legislative environment in which ISPs operate. Legislation, such as ECTA, POPIA and RICA, are all grounded in and must align with constitutional principles. The Constitutional Court's jurisprudence further influences the interpretation and application of these laws, impacting how ISPs navigate their legal obligations.

The constitutional framework of South Africa thus provides a robust foundation for the regulation and operation of ISPs. It dictates the legal boundaries within which ISPs must operate and enshrines the fundamental rights and values that ISPs must uphold in their service provision. This framework is integral in guiding the evolution of the digital landscape in South Africa, ensuring that the growth and development of the ISP industry are in harmony with the nation's constitutional commitments.

[260] Zarei et al. 2019: 199.

3.3.3 LEGISLATIVE FRAMEWORK

The legislative framework governing ISPs in South Africa is an intricate tapestry of laws and regulations that shape the operational landscape. The framework is informed by the constitutional principles of the Republic of South Africa and a series of specific statutes that address various aspects of telecommunications, cyber activities, data protection, and electronic transactions. These laws collectively establish the legal obligations and boundaries within which ISPs must operate, balancing the state's interests, the rights of consumers, and the imperatives of technological and digital advancement.

One of the cornerstone pieces of legislation in this domain is the ECT Act. The ECT Act is a pivotal law that lays the groundwork for electronic communications and transactions, setting out the regulatory framework for ISPs. It addresses a wide range of issues, from consumer protection in electronic transactions to specific provisions regarding the liability of ISPs for data hosted or transmitted through their networks. This Act marks a significant step in adapting South Africa’s legal system to the challenges and opportunities of the digital age.

Another key legislative piece is RICA. RICA sets out provisions for the lawful interception of communications and outlines the responsibilities of ISPs in this regard. It mandates ISPs to ensure that their networks can facilitate lawful interception and comply with requests from law enforcement agencies, balancing this requirement with the constitutional right to privacy and the protection of personal information.

POPIA is another critical law impacting ISPs. The POPI Act governs the processing of personal information and sets out principles for data protection that ISPs must adhere to. This includes obligations related to user consent, data security, and the reporting of data breaches. The Act aligns South Africa with international data protection standards, ensuring ISPs comply with local laws and meet global data privacy and security norms.

In addition to these specific laws, ISPs in South Africa must also navigate the provisions of the Consumer Protection Act 68 of 2008. This Act provides consumer rights and

protections in providing goods and services, including the services offered by ISPs. It covers aspects such as fair contractual practices, the provision of information, and the right to fair and reasonable marketing practices.

The legislative framework is further complemented by various policies and regulations issued by the Independent Communications Authority of South Africa (ICASA), the regulatory body overseeing telecommunications and broadcasting. ICASA's regulations and guidelines provide more detailed requirements for ISP operations, from licensing conditions to compliance with technical standards. Moreover, the framework is influenced by developments in cyber law, particularly concerning cybercrime and cybersecurity. The Cybercrimes Act 19 of 2020 is expected to provide a comprehensive legal approach to combating cybercrime, impacting how ISPs manage and report cyber incidents and their role in cybersecurity.

The Cybercrimes Act 19 of 2020 is a significant piece of legislation in South Africa that addresses various aspects of cybercrime and cybersecurity. Below is a summary of its key points:

i. Purpose:
    - To create offences related to cybercrime
    - To impose penalties for cybercrime
    - To regulate the powers to investigate, search, access, and seize related to cybercrimes
    - To regulate the jurisdiction of courts

ii. Key Offenses Defined:
    - Unlawful access to data, computer systems, and networks
    - Unlawful interception of data
    - Unlawful acts concerning software and hardware tools
    - Unlawful interference with data, computer programs, storage mediums, and systems
    - Cyber fraud, forgery, and uttering

- Cyber extortion
- Theft of incorporeal property
- Malicious communications

iii. Jurisdiction:
- Establishes jurisdiction of South African courts in cybercrime cases, including offences committed outside South Africa under certain conditions

iv. Powers of Investigation:
- Provides for search and seizure and access to data and devices
- Outlines procedures for preservation orders and disclosure of data

v. Obligations of Electronic Communications Service Providers:
- Requires assistance in investigations
- Mandates reporting of cybercrimes

vi. Establishment of Structures:
- Creates a 24/7 Point of Contact for cybercrime-related assistance
- Establishes structures to deal with cybersecurity

vii. Evidence:
- Addresses admissibility of evidence obtained through interception of data

viii. Reporting and Capacity Building:
- Mandates reporting on the implementation of the Act
- Provides for the development of human resources in cybersecurity and cybercrime detection and prevention

ix. International Cooperation:
- Facilitates cooperation with foreign states in cybercrime investigations

x. Penalties:
- Imposes fines and imprisonment for various offences, with penalties varying based on the severity of the crime

This Act represents a comprehensive approach to addressing cybercrime in South Africa, aligning the country's legal framework with international standards in cybersecurity and digital forensics. It's important to note that the implementation and interpretation of this Act may evolve over time through court decisions and amendments.

The Cybercrimes Act has several important implications for ISPs:

i. Obligations to Assist Law Enforcement:
   - ISPs are required to cooperate with law enforcement agencies in the investigation of cybercrimes.
   - They must provide technical assistance and information when served with a court order or when requested by authorized investigators.

ii. Reporting Requirements:
   - ISPs have a duty to report certain cybercrimes to the South African Police Service.
   - This includes reporting any offences under the Act that are detected on their networks or systems.

iii. Data Preservation:
   - ISPs may be required to preserve data that is believed to be involved in a cybercrime investigation.
   - They must comply with preservation orders issued by the courts or authorized officials.

iv. Access to Data:
   - The Act provides for mechanisms through which law enforcement can access data held by ISPs, subject to proper legal procedures and safeguards.

v. Liability Protection:
   - The Act provides some protection for ISPs against liability for actions taken in good faith to comply with the law or assist in investigations.

vi. Interception of Data:
   - Under certain circumstances and with proper authorization, ISPs may be required to assist in the lawful interception of data passing through their networks.

vii. Customer Privacy:

- While ISPs are required to assist law enforcement, they must also balance this with their obligations to protect customer privacy under other laws like POPIA.

viii. Infrastructure Security:
- ISPs are expected to maintain secure systems and networks to prevent cybercrime.

ix. Capacity Building:
- The Act encourages the development of cybersecurity capacity, which may involve ISPs in training and awareness programs.

x. Penalties for Non-Compliance:
- ISPs can face penalties if they fail to comply with their obligations under the Act.

It's important to note that the Act aims to strike a balance between enabling effective law enforcement in the digital sphere and protecting the rights of individuals and businesses. ISPs play a crucial role in this balance, acting as key intermediaries in the digital ecosystem.

The implementation of these provisions may require ISPs to review and potentially update their policies, procedures, and technical capabilities to ensure compliance with the Act while maintaining their service quality and protecting their customers' interests.

Related to the Cybercrimes Act and POPIA is the concept of Just In-time Processing (JIT). JIT processing in the context of cyber law primarily relates to data protection and privacy regulations. It's not a specific legal term, but rather a concept that has implications for legal compliance, especially in data protection laws like the EU's GDPR or South Africa's POPIA.

Below is an overview of Just-In-Time processing in the context of cyber law:

i. Definition: Just-In-Time processing refers to the practice of collecting, processing, or using personal data only at the exact moment it's needed, rather than storing it for potential future use.

ii. Key Principles:
    - Data Minimization: Only collect and process the data that is absolutely necessary for a specific purpose.
    - Purpose Limitation: Use data only for the specific purpose for which it was collected.
    - Storage Limitation: Retain data only for as long as necessary to fulfill the purpose for which it was collected.

iii. Legal Relevance:
    - Compliance with Data Protection Laws: JIT processing aligns with key principles in many data protection laws, such as data minimization and purpose limitation.
    - Risk Reduction: By processing data only when needed, organizations can reduce the risk of data breaches and unauthorized access.

iv. Application in Cyber Law:
    - Consent Management: Providing just-in-time notices and obtaining specific consent at the moment data is needed.
    - Privacy by Design: Incorporating JIT processing into the design of systems and processes to ensure privacy protection from the outset.
    - Data Subject Rights: Facilitating the exercise of data subject rights (like the right to be forgotten) by minimizing unnecessary data storage.

v. Benefits in Legal Compliance:
    - Reduced Liability: Less stored data means reduced risk of non-compliance and data breaches.
    - Transparent Processing: JIT processing can make it easier to demonstrate compliance with transparency requirements.
    - Easier Data Management: Simplifies the process of managing data retention periods and responding to data subject requests.

vi. Challenges:
    - Technical Implementation: Requires sophisticated systems to process data on-the-fly.

- Balancing with Business Needs: May conflict with business desires for data analytics and long-term data strategies.
- Ensuring Availability: Must ensure that necessary data is available when needed for legitimate purposes.

vii. Examples in Practice:
- Location Services: Only accessing a user's location when they use a map feature, rather than continuous tracking.
- Financial Transactions: Processing payment information only at the time of purchase, without storing credit card details.

viii. Relevance to South African Law: While not explicitly mentioned in South African cyber laws, the concept aligns well with principles in POPIA, such as data minimization and purpose specification.

Understanding and implementing JIT processing can be crucial for organizations seeking to comply with data protection regulations while minimizing cybersecurity risks. It represents a shift towards more privacy-conscious data handling practices in the digital age.

The legislative framework for ISPs in South Africa is dynamic and evolving. It reflects the ongoing effort to balance the effective regulation of a rapidly developing industry with the protection of consumer rights and the fostering of innovation and growth in the digital sector. This framework is not static; it continually adapts to new challenges and technological advancements, ensuring that ISPs operate in a manner that is lawful, ethical, and conducive to the broader socio-economic goals of the country.

3.3.4 JUDICIAL INTERPRETATION

Judicial interpretation is pivotal in shaping the operational landscape of ISPs in South Africa.[261] The judiciary's interpretation of laws relevant to ISPs clarifies legal ambiguities and significantly influences the practical application of these laws.

In South Africa, where a robust constitutional democracy characterizes the legal system, courts have frequently been called upon to interpret legislative provisions affecting ISPs, particularly in privacy, data protection, freedom of expression, and liability.

Through various landmark rulings, the South African judiciary has contributed to defining the extent and limits of ISP liability and responsibilities.[262]

In interpreting the ECT Act, for instance, the courts have had to consider the balance between the rights of internet users and the responsibilities of ISPs to control and monitor the content on their platforms. These judicial interpretations have clarified how ISPs should approach issues of illegal or harmful content hosted on their platforms, determining the circumstances under which they can be held liable for such content.

One of the critical areas where judicial interpretation has been crucial is privacy and data protection. The POPI Act and its implementation have raised significant questions about how ISPs handle personal data. Courts have had to interpret these laws to guide the extent of data protection obligations for ISPs and the ramifications of data breaches.[263] These interpretations are critical in an era where data privacy is paramount, and ISPs are often the custodians of vast amounts of personal data.

Judicial interpretation has also been significant in the context of the RICA. The courts have played a critical role in interpreting the provisions of RICA, particularly those relating to the lawful interception of communications and the extent to which ISPs are

---

261 Fernandez Nieto 2022: 7.

262 See for example Ketler Investments CC t/a Ketler Presentations v Internet Service Provider All SA 566 (GSJ), Giftwrap Trading (Pty) Ltd v Vodacom (Pty) Ltd and Others (1009/2020) [2023] ZASCA 47.

263 Dharmawan et al. 2019: 3177.

required to assist law enforcement agencies. These judicial decisions have implications for the privacy rights of individuals and the legal responsibilities of ISPs in surveillance and interception matters.

Moreover, the Constitutional Court and High Courts of South Africa have been instrumental in interpreting the Constitution in a way that impacts ISPs. Issues such as freedom of expression, access to information, and equality have all been subjects of judicial interpretation, with direct implications for ISPs. These interpretations help navigate the complex interplay between individual rights and the public interest in the context of digital communication.

The judiciary's role extends beyond mere interpretation of existing laws to address novel legal challenges posed by the evolving digital landscape. As new communication and data transmission forms emerge, courts increasingly face applying traditional legal principles to new technological contexts. This includes dealing with issues related to emerging technologies, cybercrimes, and the ever-changing nature of online interactions.[264]

3.4 INTERNET SERVICE PROVIDERS – PRESENT CHALLENGES AND LEGISLATIVE RESPONSE

3.4.1 INTERNET SERVICE PROVIDERS IN SOUTH AFRICA

South African internet users comprised 8.1 per cent of the global population of internet users in 2015, with numerous ISPs vying for consumer monopoly.[265] The South African service providers have been categorised according to relative size and governmental authorisation to provide internet services.

---

[264] Sorbán 2019: 22.

[265] Internet World Stats "African internet users November 2015" http://www.internetworldstats.com/stats1.htm (Date of use: 3 February 2016).

Three of the seven largest providers are Telkom, Neotel, and Sentech, respectively.[266] However, each year, the number of ISPs in South Africa expands. The government-directed Broadband Infraco currently regulates all ISPs.[267] Telkom, Neotel, and Sentech form the triumvirate, providing internet in the bandwidth necessary for users to move data faster and more efficiently.[268] Other service providers receive varying degrees of market share, but all must comply with the regulations imposed by the legislation mentioned above.

Indicative of the changes to costs and provisions for South Africans, for example, in 2004, two megabytes of bandwidth cost a household ZAR 250,000 or the equivalent of US$ 17,457 per month (at that time). As of 2013, the cost has dropped to a mere ZAR 637 or US$ 44 per month.[269]

The price drop elevated the number of users able to afford home internet, which increased South Africa's global reach. A caveat regarding broadband access in the home through these providers is that they all require the purchase and/or installation of a private landline to access Asymmetric Digital Subscriber Line (ADSL) services, thus restricting the ability of some users to acquire internet within the home, as the cost of the landline adds a further ZAR 30 or ZAR 40 to the overall monthly costs and some poorer families and individuals cannot meet these expenses.[270]

The advantage of ADSL internet is that users can access the internet at higher and more accurate speeds than cable or satellite technology. For users who regularly upload and

---

266 Darrynn "Bandwidth in South Africa explained" http://www.optimus01.co.za/bandwidth-in south-africa-explained/ (Date of use: 3 February 2016).

267 "South African consumer service bodies" http://www.southafrica.info/services/consumer/consumer.htm#.V4EJueR7VEA (Date of use: 1 February 2017).

268 From 80 gigabits per second to 10 Terabits per second.

269 Levinsohn "The real cost of uncapped ADSL in South Africa" http://www.bandwidthblog.com/2013/03/20/the-real-cost-of-uncapped-adsl-in-sa/ (Date of use: 1 February 2017).

270 Reddick et al. 2020: 102906.

download files, data, music, and other types of entertainment, ADSL is the most efficient and cost-effective method for accessing the internet.[271]

Telkom offers the lowest home bundle costs for internet and landline access, but the other service providers offer competitive bundles. WebAfrica's services were found to be the most expensive. Some of these providers granted the option for selecting a 1MB or a 2MB of bandwidth, whilst others gave only the 2MB availability preference.[272]

These figures and bandwidth access refer to 2013 figures and relate to broadband internet combined with mandatory ADSL,[273] which transmits data through telephone lines.

3.4.2 SOUTH AFRICAN INTERNET USE IN THE GLOBAL CONTEXT

The apparent advantages of internet capabilities are often overshadowed by the problems arising from easy and free access to the so-called "*information highway*." Data is transmitted and received constantly, with opportunities to access the daily news, shop online, and engage in global communication. Still, the flow of data also brings about the risks of invasion of privacy, computer hacking, pornography distribution, the exploitation of children, entrapment, extortion, pyramid schemes, and other forms of cybercrime.

Governmental and legal intervention is necessary to curb the harmful actions on the part of individuals or groups who may be involved in the aforementioned acts of cybercrime. Another factor is to ensure that the ISPs comply with legal parameters for the protection of their users and that corporations do not abuse their power over individuals, other

---

271 Levinsohn "The real cost of uncapped ADSL in South Africa" http://www.bandwidthblog.com/2013/03/20/the-real-cost-of-uncapped-adsl-in-sa/ (Date of use: 14 February 2016).

272 Levinsohn "The real cost of uncapped ADSL in South Africa" http://www.bandwidthblog.com/2013/03/20/the-real-cost-of-uncapped-adsl-in-sa/ (Date of use: 14 February 2016).

273 Levinsohn http://www.bandwidthblog.com/2013/03/20/the-real-cost-of-uncapped-adsl-in-sa/ (Date of use: 14 February 2016).

companies, and governments, relying on the safety and cost-effectiveness of the internet as a product.

As discussed briefly in the introduction, the applicable laws limit the government's ability to exercise control over the internet by outlining the conditions under which it can exercise its powers.

Section 31 of the ECTA outlines the parameters under which the government can exercise its authority over cryptography providers.

Section 31(2) outlines the exceptions to the rule, preventing the DG from disclosing information to third parties, like security agencies.

Section 31(2) states that the bar on disclosing information on cryptography providers does not apply in five situations. These restrictions mean that the South African State cannot ban or request information that the companies categorise as trade secrets or proprietary information.

In other countries,[274] the legislature gives the executive complete control over the internet and telecommunications companies that provide internet services to consumers and organisations within their jurisdiction. These countries have complete jurisdiction in telecommunications for many reasons.

One of the main reasons leading to the legislative extension of state power is the country's governance system. Where the country uses dictatorship as its preferred system of governance, the government uses its control over the legislature to force it to enact laws that give it complete control over the internet and ISPs.

For instance, countries run by dictatorships practice absolutism when determining the amount of information citizens may access, thus limiting access to websites. Often, this

[274] For example, China, Beijing, Bangladesh, Iran, North Korea, and Syria.

is for the government's protection, and in China, for instance, the government refused to allow Facebook until recently.[275]

The Chinese government banned access to Facebook based on the opinion that to have its people connected to citizens from countries where constitutions allow freedom of speech and different political ideologies would not be in the government's best interest. In the aftermath of pro-democracy protests in Hong Kong in 2014, China instituted a ban on foreign cryptography providers reluctant to comply with the government's edicts to tighten its control over the internet.

The Chinese government used its authority to block people in Hong Kong and mainland China from accessing WhatsApp's cryptography services (as previously discussed). The Chinese government tightened its control over ISPs and content providers by instituting a partial block on the WhatsApp platform.

However, the ban on WhatsApp has done nothing to prevent tech-savvy youth from accessing WhatsApp, Facebook, Twitter, YouTube, and other cryptographic platforms.[276] With outside pressure and the ability of hackers to circumvent government restrictions, the number of young people in China who illegally use Facebook changed this opinion, and the laws were amended.

Currently, China's population connecting to this social media site comprises 48 per cent of the total 55 per cent of those logging on to the internet.[277] China's example provides a contextualisation for the situation in South Africa. China is home to Asia's most significant internet users, and Asian users constitute 48.4 per cent of the world's internet users.[278]

---

275 2013.
276 Duffett et al. 2019: 604.
277 http://www.pewglobal.org/2014/02/13/emerging-nations-embrace-internet-mobile-technology/ *Pew Research Center* (Date of use: 26 June 2016).
278 http://www.internetlivestats.com/internet-users/ *Internet Live Stats* (Date of use: 26 June 2016).

3.4.3 LEGAL REGULATION OF INTERNET USE AND FUNCTIONING IN SOUTH AFRICA

In 2002, South Africa passed the Electronic and Communications Bill, subsequently amended in 2012 to embrace the rapidly growing and expanding global communication networks. The 2012 Amendment recognises the significance of the revisions taking place in all fields of communication and aims to promote the following:

> [E]lectronic transactions nationally and internationally, recognising the benefits and efficiency of them; to build confidence in electronic communications by introducing schemes for the accreditation of authentication services and products; to help realise the economic and social benefits that can be derived through the use of authenticated services and products in secure global electronic commerce; to provide further for the use of digital signatures; to prevent abuse of information systems by among other things, cybercrime; to secure the efficient management, issue and protection of South African domain names; to encourage the use of a-government services; and to address other relevant issues.

The South African government recognised the technological revolution and the necessity of awareness of advances to remain current with local, national, and global trends. Before 1994, freedom of speech was restricted, and global sanctions were necessary to create the opportunity for a paradigm shift in South Africa.

The post-apartheid Constitution enshrined ideological paradigms, enabling changes in South Africa—one of these changes contained in the Bill of Rights is freedom of expression. In 1996, however, the internet was still in its infancy, and its local- and global potential was yet to be realised.

By 2002, when the government passed the first Electronic Communications and Transactions Act 25 of 2002 (ECTA), the provisions sufficiently encompassed the parameters of electronic communications, including how it perceived the most efficient way of controlling the new medium. However, by 2012, the internet's capabilities and personal-, professional-, and governmental reliance on the required statute required an amendment to the ECTA in the form of the Electronic Communications Amendment Act 1 of 2014 (ECAA).

The ECAA details new definitions relating to electronic communication, provides specific guidelines for companies providing internet access, and defines every type of cybercrime and subsequent punishments for those involved in cyber-criminal acts.[279]

The intricacies of defining every mode of telecommunication are significant. South Africa is one of various nations struggling with determining how far freedom of expression infringes upon the guaranteed rights to privacy and the individual. Courts preside over numerous cases involving individuals as they interpret their rights against others regarding internet usage. This relates to the roles, responsibilities, and restrictions of ISPs because these companies face severe consequences for violating the ECTA in terms of denying rights and abusing their capacity to invade personal rights and freedoms.

3.4.3.1 KEY PROVISIONS OF THE ECTA GIVING THE GOVERNMENT AUTHORITY TO CONTROL SERVICE PROVIDERS

The definitions provision is one of the critical provisions of the ECTA on issues related to the State's authority to regulate cryptography providers and other ISPs.

Section 1 of the ECTA defines three important terms essential to an appreciation of the position of the law on the government's control over ISPs and content providers. These terms are "*cryptography service*," "*cryptography provider*," and "*cryptography product*."

Section 1 defines "*cryptography service*" by covering all the categories of services in which a company uses cryptographic techniques to ensure that the recipient of data messages, or individuals storing data messages, can limit the number of persons and organisations who can access or read the message, by controlling its intelligibility.

It also defines "*cryptography services*" as using cryptography techniques to guarantee the data's authenticity, integrity, and source.

[279] Mostly contained in the preamble and definitions section of the Act.

Section 1 of ECTA defines "*cryptography product*" as any computer software or hardware that aids the recipient or the sender of data messages using cryptography techniques to safeguard the data by controlling its intelligibility, authenticity, integrity, or source.

Section 1 of the ECTA states that "*cryptography provider*" is a phrase that denotes all persons or organisations that offer cryptography services in South Africa. This section outlines the definition of terms related to cryptography. Still, they do not provide the government with the types of powers that would allow it to prevent people from using cryptography services to threaten its interests.

The definitions are also important because they illustrate the extent of the government's authority over cryptography providers. The definition suggests that the government has authority over all cryptography providers operating in South Africa. This implies that the authority extends to all types of individuals and organisations, even when they are foreign firms and foreign nationals.

In addition to the definitions section, the Chapter on cryptography offers further guidelines on the scope of the State's authority over ISPs. More specifically, the section outlines the scope of State authority over cryptography providers. The section outlines the law regulating companies that specialise in cryptography services. Still, they do not provide the types of powers that South African security agencies require to prevent cryptography providers from engaging in activities that might undermine the legitimacy of the State.

The Chapter on cryptography providers covers sections 29, 30, 31, and 32 of the ECTA. The Chapter outlines the regulations that pertain to cryptography providers.

The first aspect of the law relates to the scope of the government's power concerning the registration of information on the activities of cryptography providers.

Section 29 of the ECTA gives the DG the authority to maintain a Register of all companies specialising in providing South Africa's cryptography services.

Section 29(2) states that the Register of those companies must include their name, address, cryptography services delivered, and other important information essential for locating the company.

Section 29(3) bars the DG from compelling service providers to disclose confidential information or any other type of information they would consider part of their trade secrets.

The law preventing the DG from compelling cryptography providers to provide proprietary information places severe limitations on the powers of the government. The law directs that the DG can only request information relating to the identity and address of cryptography providers.

However, it restricts the government's ability to collect other important information that the companies would categorise as proprietary. This restriction means that the government cannot do anything to prevent cryptography providers from operating in the country. Once the cryptography provider has complied with the law and shared information on its address, its identity, and its services, the government cannot request more information nor intervene to bar it from operating in the country because it is providing opportunities for citizens to express themselves in ways that are detrimental to the interests of the state.

The government can only react within the scope of its enacted laws.

Section 30 provides further insight into the powers of the government concerning cryptography providers that have not complied with the rules under the Chapter on cryptography providers. The section allows the government to stop such companies from operating within South Africa. Section 30 of the ECTA bars companies from delivering cryptography services within the country before they have complied with the registration requirements under section 29.

Section 30 provides three conditions under which the ECTA will regard a service provider as delivering its services within South Africa.

Section 30(3)(a) states that a company will provide cryptography services within South Africa if it delivers them from premises within the country. Section 30(3)(b) states that a person or organisation will deliver cryptography services within South Africa if it delivers its services to an individual.

Section 30(3)(c) states that a person or organisation will be delivering cryptography services within South Africa if it delivers the services to an individual or organisation that uses it for a business that operates in South Africa.

The essence of section 30 is that it outlines the scope of the application of the provisions on cryptography. It suggests that the law covers South African companies and companies registered in other parts of the world but offers cryptography services to consumers and organisations in South Africa.

The wording of section 30 suggests that South Africa has extensive powers when dealing with ISPs that have not complied with section 29. The section indicates that organisations that do not comply with the existing rules and decide to offer their services without registration will not receive the protections afforded to organisations that have complied with the section by registering their services and products. Their existence outside the legal protections means that the government can control the organisation and its activities.

The exceptions in section 31 suggest that the State has far-reaching powers regarding its control over cryptography providers. The reality, however, is that other provisions in the Chapter on cryptographies have limited State power. When one evaluates the powers of the State against other limitations within the same Chapter on cryptography providers, it becomes clear that the State's power over cryptography providers is limited.

This restriction means that the government cannot compel cryptography providers to share with them the types of information that will lead them to gain access to the encryption codes. It means that the government cannot force cryptography providers to

give them a back door into the software and hardware they use to encrypt data that people and organisations in South Africa are sending and receiving.

The law gives the South African government control over cryptography providers. Still, its provisions remove that control by limiting the State's ability to control the ISPs. This is markedly different from the situation prevailing in China, where the state controls cryptography service providers.

3.4.4 STATE ABILITY TO PROTECT CONSUMERS

The government's limited control over ISPs and content providers also manifests in the laws enacted to protect consumers from hacking, identity theft, and other categories of cybercrime. Existing provisions of the ECTA outline the scope of the government's ability to protect consumers from cybercrime.

An evaluation of the provisions suggests they are robust, but none have effectively protected South African consumers against the rising incidence of cybercrime.

Section 86 of the ECTA outlines the circumstances under which an individual will engage in cybercrime.

Section 86(1) of the ECTA states that a person engages in cybercrime when he intentionally intercepts or accesses electronic data without permission or authority.

Section 86(2) provides another definition of cybercrime when it states that a person engages in cybercrime when he interferes with electronic data in a way that destroys it, modifies it, or renders it ineffective.

Section 86(3) adds a third definition of cybercrime when it classifies the unlawful possession, distribution, adoption, procurement, sale, or design of computer programs or electronic devices in a way that influences them to access data or codes to use to violate any of the provisions of section 86 as a cybercrime.

Further, section 86(4) states that a person engages in cybercrime when he uses the program or device mentioned in section 86(3) to circumvent cyber security measures that consumers and other organisations have implemented to prevent intruders from accessing data.

Section 87 of the ECTA outlines the definitions of computer-related forgery, fraud, and extortion.

Section 87(1) states that a person commits the crime of extortion, fraud, and forgery when he threatens to engage in any of the cybercrimes defined in section 86 of the ECTA to obtain a proprietary advantage through unlawful means.

Section 87(2) states that a person commits the crimes of forgery, extortion, or fraud when he utilizes any of the crimes outlined under section 86 to cause the generation of fake data that leads other people or institutions to act on it because they believe that it is genuine data.

Each definition suggests that the existing laws have given the government the power to protect consumers against cybercrimes and cyber-criminals. However, an analysis of statistics on cybercrime indicates that the laws have not given the government adequate power to protect consumers from the activities of cybercriminals.

Statistics on cybercrime in South Africa suggest that consumers in the country are at the mercy of cyber-criminals.

Statistics from the Norton Cybersecurity Insights Report (as discussed in Chapter 2) offer further confirmation of the deteriorating state of cybersecurity in South Africa. According to the Report, researchers surveyed 18,000 consumers from eighteen countries. As a part of the study, they recruited 1,001 online users from South Africa. They used the extrapolation method to multiply the percentage of South African victims by the number of adult online users in South Africa. This multiplication allows the organisation to estimate the number of online users in the country who are victims of

cybercrime over twelve months. The study's results suggest that 8.8 million adult online users in South Africa fall victim to cybercrime.[280]

According to the results, *Generation X*-users[281] and *Millennials*[282] shouldered a disproportionate burden of cybercrime. The statistics suggest that 37 per cent of *Generation X*-users and 39 per cent of *Millennials* in South Africa fell victim to cybercrime during the twelve months of the study. The results suggest that the attacks against *Generation X*-users and Millennials were high at a time when statistics showed that South Africans had higher levels of sensitivity to cybercrimes than their counterparts from other developed and developing countries.[283]

The statistics on sensitivity to cybercrime suggest that 76 per cent of South Africans surveyed knew about the spike in the rate of online identity theft, and 67 per cent of the South Africans surveyed knew about the strategies that they could implement to control the loss of their personal information over the internet. Despite the high degree of sensitivity towards cybercrime, South Africans were still falling victim to cybercrime.[284]

Furthermore, 31 per cent of the Millennials surveyed in the study stated that they felt it was more convenient to abandon their online accounts instead of deleting them.[285]

An example of the problematic state of ISP regulation relates to freedom of expression. This is no more obvious than in the use of Facebook. The South African courts support

---

280 Norton Life Lock "2021 Norton Cyber Safety Insights Report" https://www.nortonlifelock.com/us/en/newsroom/press-kits/2021-norton-cyber-safety-insights-report/ (Date of use: 12 August 2022).

281 Ibid n215.

282 Ibid n216.

283 Norton Life Lock "2021 Norton Cyber Safety Insights Report" https://www.nortonlifelock.com/us/en/newsroom/press-kits/2021-norton-cyber-safety-insights-report/ (Date of use: 12 August 2022).

284 Norton Life Lock "2021 Norton Cyber Safety Insights Report" https://www.nortonlifelock.com/us/en/newsroom/press-kits/2021-norton-cyber-safety-insights-report/ (Date of use: 12 August 2022).

285 Norton Life Lock "2021 Norton Cyber Safety Insights Report" https://www.nortonlifelock.com/us/en/newsroom/press-kits/2021-norton-cyber-safety-insights-report/ (Date of use: 12 August 2022).

the countries[286] that guarantee freedom of expression in attempting to resolve the dilemma of which right takes precedence when weighing state security, protection of citizens and the right to freedom of expression.

No restrictions exist over the legality of Facebook as a legitimate form of social media. Therefore, ISPs in South Africa do not block unrestricted use of Facebook. *H v W*,[287] a recent case before the South Gauteng High Court, illustrates the complexity between competing rights, especially freedom of expression, and the legal parameters.

In February 2012, the respondent posted a letter on Facebook bringing to "*public consumption*" negative and inflammatory remarks about the applicant. The primary discussion of the arguments centred upon privacy versus the right to public information since both parties belong to Facebook.

The applicant argued that the posting harmed his reputation in the community and business and publicised his marital difficulties. Even though the two parties had been friends for many years, the litigant's attorney stated that their friendship did not privilege the respondent to make intimate personal affairs public on a social media platform.

The respondent's attorney reverted to the Code of the Byzantine Emperor, Justinian, and his *Corpus Iurus*, in which the common law allows for both the right to privacy and freedom of expression. The respondent's case continued with a detailed history from the Justinian era to the Dutch legalists, whose laws also respected privacy and freedom of expression, to the notable changes the electronic age of communication and social media, such as Facebook, continue to create.

The respondent's attorney noted that Facebook continually updates its privacy policy and allows its members to inaugurate a privacy button on their site so that only friends can see their posts. It was argued that it is the member's responsibility to change

286 For example, United States, Libya, and Cuba.
287 *H v W* 2013 2 SA 530 (GSJ).

personal profiles and activate privacy buttons; therefore, freedom of expression is allowable via this social medium.

A year later, the case was decided in favour of the applicant. The arguments presented emphasised that all individuals are entitled to "*dignitas"* (inner tranquillity) and "*fama"* (reputation).[288]

The respondent was ordered to remove all such postings from Facebook and other social media and pay the applicant's costs.[289] In reaching its final decision, the Court reminded the public that a similar case[290] noted that:

> the question of whether private sectors are worthy of protection is determined by reference to 'ordinary or reasonable sensibilities'… and the law is not concerned with trivia[.][291]

This implies that the invasion of privacy and reputation is beyond trivial matters and must be taken seriously.

Since 2014, over 62 per cent of South Africans have engaged in social media, and as of 2015, more than 13,000,000 citizens are on Facebook alone, discounting LinkedIn or Twitter. Therefore, the viability of the Court's decision relating to *dignitas* appears appropriate.[292] Within this context, the need to understand the participation and responsibility of ISPs becomes relevant.

The ECTA attempted to address the accreditation and registration of those offering products and services in addition to encryption and cryptography capabilities. The ECTA was, however, instituted before the creation of Facebook, Twitter, and LinkedIn. However, after 2004 and Facebook's inception by Mark Zuckerberg, Facebook

---

288 *H v W* 28.
289 *H v W* 28.
290 *National Media v Joost* 1996 3 SA 262 (SCA).
291 *H v W* 28-29.
292 http://www.pewglobal.org/2014/02/13/emerging-nations-embrace-internet-mobile-technology/ *Pew Research Center* (Date of use: 15 February 2016).

participation escalated rapidly, reaching nearly 172,000,000 million members globally. This phenomenon creates a problem for courts, governments, and ISPs.

Based on the United Nations General Assembly and Civil Rights Council Report, a comparative issue may be raised regarding the right to privacy versus freedom of expression.[293] This Report presents several problems and issues relating to the ultimate determination of the amount of power to be given to ISPs and the effect of this power concerning privacy and freedom of expression.

The Report focuses on numerous countries with constitutional provisions relating to freedom of speech (expression), such as the USA, Canada, the UK, the EU, and South Africa. The problem of judging freedom of expression against the rights of individual and/or governmental privacy must be determined through legal and legislative means to prevent violations by rogue hackers or those who consider that all information in the public domain belongs to any individual or group.

3.4.5 INTERNET SERVICE PROVIDERS IN SOUTH AFRICA

According to the ECAA, ISPs have an extensive responsibility relating to how internet services are offered to both the private- and public sectors. The South African internet network is expanding annually. Since 2012, this network has been 99.9 per cent digital, which includes the latest, fastest, and most inclusive internet communication networks. This renders South Africa's system the most advanced and sophisticated on the African continent.[294]

This type of communication system comprises various legal responsibilities and the social-, cultural-, and economic responsibilities presented in its governing legislation—

---

293 UN HRC (16 May 2011) *La Rue F Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression Human Rights Council 2011 UN Doc*. A/HRC/17/27 59-69.

294 http://www.southafrica.info/services/consumer/consumer.htm#.V4EJueR7VEA (Date of use: 1 March 2018).

the South African legislative parameters detail how these ISPs must comply with the country's laws.

Legally, ISPs have several guidelines, particularly regarding illicit activity carried on by any of its subscribers. With the combined efforts of the South African government and Telkom-, MTN-, Vodacom-, Cell C-, and 8ta ISPs, the smooth-running fibre-optic networks offer faster speeds and the best designs for connectivity.

Relative to this legitimate communication networking, the underside of illegal activity keeps the courts involved in litigation, similar to other countries facing the current difficulties regarding the latest technology and the law. The advances of cybercrime occupy the courts and the legislature in attempting to understand, control, and effectively judge between factors relating to the constitutional guarantees of freedom of expression and the right to privacy.[295]

3.4.6 THE IMPLEMENTATION OF THE ECAA

The ECAA attempts to define further cybercrime, the legal consequences imposed for violations, and the responsibilities of ISPs within these violations.

Within the areas of cyber responsibility and according to the ECAA, the most significant of these are discussed as they relate to both the ISPs and their subscribers.

3.4.6.1 AMENDMENTS TO SECTION 2 OF THE ECT ACT

The amendment of section 2 of the ECTA acknowledges that the cyber world is evolving and that the ECTA was insufficient to protect consumers from technology's encroachment on the world of communication. The section outlines that the ECAA ensures and facilitates communication to all areas of the country and all citizens by overseeing how telecommunications are distributed.

[295] La Rue 2011 UN Doc. A/HRC/17/27 59-69.

ISPs must "*promote universal access; remove barriers to electronic service; and promote legal certainty and confidence in electronic transactions*."[296]

Each subsection presents the parameters expected of accredited ISPs to guarantee that users will have their privacy protected in all transactions, regardless of where they live in South Africa.

Building a nationwide cyber-structure is an ongoing effort among ISPs, posing specific difficulties. For instance, the State-owned internet overseer Broadband Infraco has the task of "*selling high-capacity long-distance transmission services to telecom operators, ISPs, and other value-added network service providers*"[297] to lower the price to consumers for acquiring these services.

Because South Africa comprises many rural areas, a variety of national languages, and cultural diversity, the major ISPs have taken separate responsibilities for complying with the mandates in the ECAA. These responsibilities include the efforts of MTN, Noetel, and Vodacom to construct a 5,000-kilometre fibre optic system in major centres across the country, as well as the construction of a fibre telecommunications building, and the implementation of a 12,000-kilometre fibre optic communications network.[298]

Connecting South Africans to the internet will help to maintain South Africa's presence within the global community economically, politically, and socially. The economic benefits may be measured through various marketplaces that consumers and merchants can access. Government links could ease the burden of some in outlying villages to transact business or merely communicate with the government via the Internet.

---

296 See the Electronic Communications and Transactions Amendment Bill (hereinafter "ECTAB") as published in the Government Gazette No. 358211-69 (26 October 2012).

297 http://www.southafrica.info/services/consumer/consumer.htm#.V4EJueR7VEA (Date of use: 23 March 2016).

298 http://www.southafrica.info/services/consumer/consumer.htm#.V4EJueR7VEA (Date of use: 23 March 2016).

Section 2 of the ECAA states that the internet " promotes *the development of electronic transactions services which are responsive to the needs of users and consumers*".[299]

Another positive facet of the ISPs' responsibilities advises that "*the special needs of particular communities and areas and the disabled are duly taken into account*."[300] The humanitarian aspects and value of the Internet are essential to understanding the overall telecommunication complexity. Involving a nation in this form of communication and technology vitally supports the growth of a country whilst simultaneously involving every citizen, regardless of proximity, to the significant hubs or government centres in terms of the country's global image.

3.4.6.2 AMENDMENT OF SECTION 28 OF THE ECTA

Cryptography and the ability to encrypt data are becoming essential for internet users to understand and for ISPs to adopt. When individuals and/or groups supply personal data, they have only the guarantee of the ISPs that their information is encrypted to block others from stealing personal information.

For several years, cyber theft and hacking have required intervention by governments, ISPs, groups, and individuals whose vital and private details have been stolen. The courts are faced with assessing how much damage any group or person suffers when their personal information is stolen. Governments must determine the next set of regulations to prevent this theft.

When Julian Assange, for example, used the power of the internet to release thousands of delicate documents, his actions incited several years of investigation, scandal, and opposition to this type of freedom on the internet. Edward Snowdon (another example) took advantage of his position as a minor programmer working for the US State Department and released documents that might have risked several individuals' lives.

---

299 ECTAB GG No. 358211-69 (26 October 2012) 11.
300 ECTAB GG No. 358211-69 (26 October 2012) 11.

The actions of these two men ignited global controversy. Assange remains a political refugee in the Bolivian Embassy in London, and Snowdon sought and received asylum in Russia. These two individuals perpetrated the release of data on the internet, from cyberspace to the world, and once information is made available on the internet, it cannot be recalled.

Assange and Snowdon sparked a legal debate, as arguments can be made for the philosophical stance that all information is meant for public consumption. On the other hand, the government asserts that some classified details cannot be released to the public for fear of falling into the hands of terrorists.

The question arises whether the affected government could necessarily shut down all ISPs, thus achieving the right of privacy and preserving governmental secrets whilst subsuming freedom of expression. Does the ultimate responsibility lie with the ISPs to control every piece of information on the internet? Assange and Snowdon could not have acted as they did without ISPs.

In South Africa, according to the ECTAB, no service provider can offer goods, in this case, access to the internet, without specific ministerial accreditation. The ECTAB allows the government to deny accreditation, but the short- and long-term ramifications of this type of action are vast.

Removing every internet site would isolate South Africa, or any country, from connectivity to the global marketplace.[301] Governments would come to a virtual halt. Every industry would collapse without access to the Internet. Present-day corporations, governments, schools, individuals, and virtually every entity rely on Internet access. Thus, ISPs in South Africa and every other country hold the country's economic power

[301] Comninos https://www.apc.org/en/system/files/Intermediary_Liability_in_South_Africa-Comninos_06.12.12.pdf (Date of use: 30 June 2016); see also "Request a take-down notice" 2016 *Internet Service Providers Association* http://ispa.org.za/code-of-conduct/request-a_take-down/ (Date of use: 29 June 2016).

in their corporate hands. In his Report to the UN, La Rue notes that the internet is the most powerful tool of the twenty-first century.[302] This is an undeniable observation.

In South Africa, the amendment to section 28 of the ECTA refers to the necessity of private and public information, cryptography, and the rights of governments and individuals. In La Rue's extensive Report to the Human Rights Council,[303] he observed that although information should be freely obtainable on the Internet, two caveats should apply:

> The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may, therefore, be subject to certain restrictions, but these shall only be such as are provided by law and are necessary: (d) for respect of the rights or reputations of others; (e) for the protection of national security or of public order (*ordre public*), or of public health or morals.[304]

These restrictions imposed on the availability, or the rights, of the public to access all information are dealt with by the courts and the national legislature.

One of the issues in South Africa is the lack of encryption laws in the country. Although the ECTAB addresses specific parameters meant to ensure the privacy of internet users, the question of who determines "*cryptography providers*" requires consideration. The explanatory memorandum to the ECTAB indicates that the purpose of Chapter 5 is to address the government's security concerns.

Comments from one of the country's respected cryptography lawyers, Lance Michalson, pose several questions about the cryptography issue in South Africa. If a cryptography provider fails to register with the Ministry, the provider (or its representatives) will be fined or imprisoned. Notably, the ECTAB fails to denote who is a provider. Another issue is that no cryptography products are currently available in South Africa. This raises the question about cyber security for those entrusting personal data to the invisible "other"

---

302 La Rue 2011 UN Doc. A/HRC/17/27 7.
303 La Rue 2011 UN Doc. A/HRC/17/27 59-69.
304 La Rue 2011 UN Doc. A/HRC/17/27 7.

through the internet. If no crypto protection is obtainable, what assurance do users have that their ISP acts in their best interests according to the ECTA and the ECAA?

3.4.6.3 AMENDMENT OF PART 2 OF CHAPTER VI OF THE ECTA

A further compliance order for ISPs through the ECTA and its counterpart ECAA relates to the accreditation and registration of these ISPs by an authorised ministry or other entity designated under the ECAA. To operate as an ISP in South Africa, every provider of internet services must become accredited through a ministerial agency. Failure to do so could result in severe financial penalties and possible imprisonment. Those ISPs who refuse to comply with orders to meet standards for accreditation and authorisation will be fined and their officers imprisoned for varying lengths of time, not exceeding one year.

This provision sets the regulatory parameters for ISPs.[305] Lack of compliance indicates a form of cybercrime, but it is necessary to address the ISPs' views that they function as an entity with a law unto itself. These parameters are instituted to protect internet users from individuals like Assange or Snowdon (who may believe the ultimate results of their actions are justifiable, regardless of acting outside of the law, without consent, and with individual determinations relative to the morality of their deeds).

However, it is necessary to note that ISPs have remained available to them. This raises questions of whether the ISPs may have been complicit in the distribution of information and whether the removal of the ISPs would have contradicted the respective governmental agencies' best interests.[306]

3.4.6.4 AMENDMENT OF CHAPTER IX OF THE ECTA

Following the aforementioned premise regarding the government's responsibility and ISPs' compliance with the regulatory provisions within the law, Chapter IX and its

[305] Bagraim 2010:101.
[306] Mphidi 2008: 7.

subsequent amendments pertain to the "*protection of critical information [databases] and critical information infrastructure*."

This amendment protects South Africa's and its citizens' national security. Critical information refers to similar data that Assange and Snowdon determined as belonging to the public domain and encompasses the view that the government has no rights to privacy.

Snowdon risked the people's lives by exposing specific individuals to various aspects of US State Department data. The US State Department served as its own ISP and was, therefore, able to shut itself down to protect the exposed individuals. The legal question, however, remains that if Snowdon had used other ISPs to disseminate his US State Department secrets, would the government have the right to order the universal removal of all ISPs? Furthermore, this raises the question of whether these cases must be dealt with through the judiciary, regardless of the immediate effect of these actions.

Chapter XI offers ISPs a "*safe haven*" against various liabilities caused by technical difficulties or the misuse of their services by users disregarding Internet law. This legislative safeguard for ISPs comes with the condition that if the provider(s) do not comply with the ministerial directives regarding licensure, accreditation, and other rules established for ISPs, then the limited liability protection offered by the government will become invalid.[307]

Since the regulations are established in the ECTAB, ISPs must ensure they know all the specifics of the Amendment. In South Africa, the law specifically and clearly states that ISPs must audit their members and provide the government with data relating to the types of information stored in its databases.[308] However, this amendment creates more questions than answers.

---

307 ECTAB GG No. 358211-69 (26 October 2012) 51.

308 Farelo & Morris "The status of e-government in South Africa" http://researchspace.csir.co.za/dspace/bitstream/10204/966/1/Farelo_2006_D.pdf (Date of use: 29 June 2016).

The amendment further allows the Ministry to demand periodic audits with severe penalties for non-compliance (a fine of ZAR 5 million and up to three years imprisonment for its Chief Executive or other representative). Suppose, however, an individual or group accesses vital governmental information and leaks it online. In that case, auditing does not stem the tide of information; it merely discovers what data types threaten national security.

3.4.7 EDUCATION AND THE INTERNET

Despite the government's difficulties regarding the internet and its providers, many positive activities are funded and supported by ISPs.[309] An example is the reward and support of South African teachers who take advantage of the ISPs' Association's (ISPA) generosity in bringing ICT to teachers. The ISPA annually offers a Super Teacher of the Year, emphasising ICT. Recipients of this award have noted that they took advantage of the ICT training and inserted the ideas into their classrooms.

By importing ICT into classroom environments, one teacher, the winner of the 2015 ISPA Super Teacher Award, Mabore Lekalakala of Toronto Primary School, stated:

> [H]er classroom is much more than the physical four-walled structure, and that her learners and she herself have become part of a huge virtual classroom that extends far beyond the confluence of her community.[310]

Education and educational services are afforded opportunities in the age of telecommunications. Rural schools like those in South Africa now have access to a global educational environment. Rural students can associate with students worldwide via internet capabilities.

---

309 Okai-Ugbaje et al. 2020: 49.

310 "ISPA super teacher of the year is today South Africa's foremost ICT in education competition for teachers" http://ispa.org.za/press-release/ispa-superteacher-of-the-year-is-today-south_africas-foremost-ict-in-education-competition-for-teachers/ (Date of use: 13 February 2016).

To date, the CoZa Foundation,[311] in conjunction with the ISPA and its Train the Teacher Program, has endowed over 5,000 teachers with ICT training, ensuring the continued progress of South African Teachers and the advancement of students in ICT learning.

3.4.8 INTERNET SERVICE PROVIDERS AND E-GOVERNANCE

The Internet and ISPs have altered the exchange of private and public communication, and the government has become the most prevalent user of Internet protocols. Local, national-, and international communication falls under the ambit of e-governance in how the government communicates with its citizens. Therefore, eGovernance ensures the transmission of accurate data and the assertion of benefits to citizens through this medium.

The government suggests that the use of e-government services provides easy access to necessary information, is convenient to use, affords better customer service, reduces the cost of doing government business, and thus lessens the taxpayer's burden by, for example, reducing paperwork (another taxpayer savings).[312] An additional advantage to e-governance is to drive lesser economies to first-world economic diversity, which is one of the visions of the political leaders in South Africa.[313]

The successful implementation of e-governance requires providing the most efficient, believable, and trustworthy services to the country's taxpayers and internet users. Reporting on information from the WSIS, South African leaders suggest that through commitment, cooperation, and diligence, the government can elevate itself into becoming a first-world economic competitor.[314]

---

311 CoZa Care Foundation is a non-profit organisation in Johannesburg.

312 "E-Government for service delivery" http://blog.bcx.co.za/1087/egovernment-service-delivery/ (Date of use: 25 June 2016).

313 Farelo & Morris http://researchspace.csir.co.za/dspace/bitstream/10204/966/1/Farelo_2006_D.pdf (Date of use: 29 June 2016).

314 Farelo & Morris http://researchspace.csir.co.za/dspace/bitstream/10204/966/1/Farelo_2006_D.pdf (Date of use: 29 June 2016).

There are two pertinent questions regarding South Africa's ability to attain successful e-Governance. First, is there sufficient leadership within the government to promote e-government? Second, how will this program be measured and managed? The individuals who aim to act on the WSIS vision require guidelines regarding the effect of e-governance on the government's relationship with the private sector, specifically in terms of privately owned ISPs. Another question is how this type of governance should be communicated to the public and whether it will be accepted.[315]

3.4.8.1 INTERNET SERVICE PROVIDERS AND E-GOVERNANCE

The prospect of e-governance is complicated because many South Africans cannot afford internet access. Furthermore, the potential lack of education of citizens living in rural areas means a lack of technological skills to access the internet, as computer literacy is a prerequisite for internet use. Rural townships may not yet be equipped with broad-bandwidth services, and all the national languages are not represented on the internet for users who are not fluent in English.[316]

In 2015, Minister Radebe, as part of an ICT Summit, discussed the significance of putting South Africa in the top tier of internet and e-government use to align the country with the top economic market countries. He notes that although, in 2013, 40 per cent of the world's population had access to the internet, the entire African continent only had an estimated 27 per cent penetration of internet access and use.[317]

This demonstrates the need for African countries to improve their technological systems. He encourages the advancement of adequate education in ICT and the cessation of corruption of government personnel, distributing rights to corporations, and the theft of

---

315 Farelo & Morris http://researchspace.csir.co.za/dspace/bitstream/10204/966/1/Farelo_2006_D.pdf (Date of use: 29 June 2016).

316 Radebe "Gauteng e-Government and ICT Summit 2015" http://www.gov.za/speeches/minister-jeff-radebe-gauteng-e-government-and-ict-summit (Date of use: 26 June 2016).

317 Radebe "Gauteng e-Government and ICT Summit 2015" http://www.gov.za/speeches/minister-jeff-radebe-gauteng-e-government-and-ict-summit (Date of use: 26 June 2016).

equipment meant to enhance the government's internet use.[318] For these programs to be developed following the world's premier economic and technologically advanced countries, Radebe notes that:

> Governments are challenged to re-examine the way their organisations and processes are structured and to identify opportunities for integration and simplification to reduce service delivery costs, minimise the burden of accessing services from citizens, and thus increase citizen-satisfaction. Governments and departments that do not embrace ICT are bound to falter in their service delivery mandate.[319]

The most efficient way for the government to provide South Africans with internet access is to ensure that the ISPs follow the government directives instituted in the ECTAB. Radebe further states that:

> Governments are challenged to re-examine the way their organisations and processes are structured and to identify opportunities for integration and simplification to reduce service delivery costs, minimise the burden of accessing services from citizens, and thus increase citizen-satisfaction. Governments and departments that do not embrace ICT are bound to falter in their service delivery mandate.[320]

3.5 PRELIMINARY CONCLUSION

It is imperative to reflect on the intricate interplay of historical, constitutional, legislative, and judicial dimensions that shape the role and liability of ISPs in South Africa. This chapter has navigated the evolving landscape of ISP regulation, highlighting the challenges and responsibilities of ISPs in the contemporary digital era.

---

318 Radebe http://www.gov.za/speeches/minister-jeff-radebe-gauteng-e-government-and-ict-summit-2015-2-nov-2015-0000 (Date of use: 22 June 2016).

319 Radebe http://www.gov.za/speeches/minister-jeff-radebe-gauteng-e-government-and-ict-summit-2015-2-nov-2015-0000 (Date of use: 22 June 2016).

320 Radebe http://www.gov.za/speeches/minister-jeff-radebe-gauteng-e-government-and-ict-summit-2015-2-nov-2015-0000 (Date of use: 22 June 2016).

The journey of ISPs in South Africa from the pre-constitutional era to the present reflects a significant transformation influenced by the country's political and social evolution. Initially, the telecommunication sector was characterized by state control and limited competition. However, the post-constitutional era marked a liberalization wave, introducing competition and innovation within the ISP industry. This historical evolution is a narrative of technological advancement and a story of aligning with democratic values and the principles of open access and information dissemination.

The Constitution of South Africa, particularly the Bill of Rights, has been pivotal in shaping ISP operations. It guarantees rights such as privacy and freedom of expression, which are fundamental to ISP activities. Legislation like the ECT Act, POPI Act, and RICA, rooted in constitutional principles, provide a structured legal framework for ISP operations, ensuring a balance between user rights, national security, and the open flow of information. The legislative framework has evolved to address emerging issues like cybercrime, data protection, and the need for a competitive yet fair marketplace.

South African courts have played a crucial role in interpreting laws affecting ISPs, providing clarity and direction in data protection, content regulation, and ISP liability. These rulings are instrumental in guiding ISPs in complying with legal requirements while respecting the constitutional rights of their users.

ISPs in South Africa face various contemporary challenges, including cybersecurity threats, the digital divide, and the rapid pace of technological change. Legislative responses, though robust in intent, face practical difficulties in implementation. As seen in the ECT Act amendments, the government's approach reflects a commitment to adapt and respond to these evolving challenges. However, the effectiveness of these legal frameworks in practice remains a matter of ongoing evaluation and refinement.

South Africa's alignment with international standards and obligations, such as those set by the ITU and under the GDPR, reflects a commitment to maintaining global best practices in ISP regulation. This alignment is crucial for ensuring South African ISPs

operate within a worldwide internet governance framework, addressing issues like cross-border data flow, cybercrime, and digital rights.

ISPs have a significant role in facilitating e-governance and bridging the digital divide. The government's push towards e-governance underscores ISPs' need to provide reliable and inclusive services. Efforts to expand internet access to rural and underserved areas are about technological expansion and ensuring social inclusion and equitable access to information.

Looking ahead, the ISP industry in South Africa faces both opportunities and challenges. Digital transformation, accelerated by global trends and local demands, opens new avenues for ISPs to innovate and expand their services.[321] However, this also calls for a vigilant and adaptive regulatory approach. There is a need for continuous dialogue among stakeholders, including ISPs, the government, judiciary, and civil society, to ensure that the regulatory environment remains responsive and effective in addressing the dynamic nature of the digital world.

In the next chapter, the researcher examines the role and liability of ISPs in China to demonstrate the extreme other end of the liability debate and to examine if any specific lessons can be helpful for the South African control and regulation of ISPs.

[321] Mhlanga & Moloi 2020: 180.

CHAPTER FOUR

THE ROLE AND LIABILITY OF INTERNET SERVICE PROVIDERS IN CHINA

4.1 INTRODUCTION

The digital age has dramatically transformed how societies interact, conduct business, and govern. ISPs are central to this transformation, which has become pivotal in shaping the digital landscape.[322] This chapter embarks on a comprehensive examination of the role and liability of ISPs in China. The analysis aims to delineate the distinctive features of China's ISP regulatory framework and draw insightful comparisons with the South African context. The objective is to uncover potential lessons and effective practices that could be beneficial for enhancing South Africa's approach to ISP regulation.

China presents a particularly intriguing case study due to its unique socio-political environment and its approach to internet governance. Unlike liberal democracies, where freedom of expression and privacy are often paramount, China's governance model significantly emphasises state control and information regulation. This starkly different stance provides fertile ground for exploring how ISPs operate under stringent regulatory frameworks and what implications this has for their roles and liabilities.

The chapter commences by delving into the historical development of ISPs in China. This exploration is crucial as it lays the foundation for understanding the current regulatory landscape. China's journey with ISPs began in the 1990s, marked initially by state control and gradual liberalization. Tracing this trajectory reveals how the interplay between political imperatives and economic considerations has shaped the evolution of ISP regulation in China.

322 Wu 2003: 141.

The chapter discusses contemporary themes and issues surrounding Chinese ISPs following the historical context. This section is vital for grasping the complexity of the current regulatory environment. It examines international obligations, the constitutional framework, legislative structures, and judicial interpretations. Each aspect plays a significant role in defining the operational and legal boundaries for ISPs in China.

One of the most compelling aspects of the Chinese context is the balance—or tension—between adhering to global Internet governance norms and enforcing stringent domestic regulations. This dynamic is particularly pronounced in content censorship, cybersecurity, and data protection areas. How Chinese ISPs navigate these dual obligations offers valuable insights into the complexities of internet governance in a rapidly evolving digital world. Furthermore, understanding China's constitutional and legislative frameworks is indispensable for comprehending the broader context in which ISPs operate. The Chinese model, characterized by an overarching state authority over digital communications, contrasts with more liberal regulatory regimes. This contrast allows for critically examining different governance models and their implications for ISPs' roles and liabilities.

Moreover, the chapter will explore how Chinese courts have influenced ISP operations by interpreting relevant laws. Judicial rulings in China often have far-reaching implications, especially in a system where legal provisions related to the Internet are subject to varied interpretations. Analysing these interpretations offers an understanding of the practical application of laws and the challenges ISPs face in compliance. Lastly, the chapter will address the present difficulties and the legislative response in China's ISP sector. This section is crucial for understanding how the regulatory framework is applied in practice and the effectiveness of the Chinese government's strategies in regulating ISPs. It will show the balance China strives to maintain between fostering technological innovation and exercising control over the digital space.

4.2 INTERNET SERVICE PROVIDERS – HISTORICAL DEVELOPMENT

China's journey in ISPs is marked by unique characteristics, primarily influenced by its political structure and approach to information control. The early development of ISPs in China can be traced back to the 1990s when the internet was introduced as a novel technology. Initially, the focus was on academic and government use,[323] with the commercial aspect of internet services evolving slowly. The state, recognizing the potential of this modern technology for economic development and international connectivity, played a crucial role in its propagation.

During these early stages, the Chinese government established a robust regulatory framework with significant state control and oversight. This was done to ensure that the burgeoning internet space aligned with the broader socio-political goals of the state.[324] The government established several state-run ISPs tasked with providing internet services while adhering to strict regulatory guidelines. These ISPs operated under the watchful eye of various governmental agencies, ensuring compliance with national policies and regulations.

As the internet began to gain popularity and its potential for economic growth became evident, China gradually liberalised its ISP market. This period saw private players and foreign investments enter, albeit within a tightly regulated framework. The government's approach was to foster competition while retaining significant control over the content and quality of internet services.[325]

This era of liberalization led to a rapid expansion of internet infrastructure and services across China. The number of internet users soared, and ISPs began offering a more comprehensive range of services, including broadband and mobile internet. However,

323 Wu 2003: 142.
324 Yoo 2006: 1847.
325 Wu 2003: 141.

the growth of ISPs in China was a story of technological advancement and a narrative of how the state navigated the challenges of maintaining control in a rapidly evolving digital landscape.

The regulatory environment during this period was marked by the implementation of various laws and policies to govern internet content, cybersecurity, and data protection. ISPs were required to adhere to strict content filtering guidelines and held accountable for disseminating prohibited information. This period also saw the strengthening of the “Great Firewall of China,” a term used to describe the country's sophisticated internet censorship and surveillance system.[326]

In the contemporary context, ISPs in China operate within one of the world's most complex and dynamic digital ecosystems. The state's role in the ISP industry has evolved to balance economic growth, technological innovation, and information control objectives.[327] ISPs are not only providers of internet services but also key players in implementing the state's digital policies.

The current landscape is characterized by the dominance of several large ISPs, many of which have expanded their services to include digital content, e-commerce, and cloud computing.[328] While operating in a competitive market, these ISPs are still subject to stringent regulatory requirements, especially concerning content control and user data protection.

Global trends and challenges, such as cybersecurity threats and the need for data sovereignty, have also influenced China's approach to ISP regulation in recent years. The government has implemented various measures to enhance the security and reliability of Internet services, placing additional responsibilities on ISPs. These include

326 Yoo 2006: 1847.
327 Wu 2003: 142.
328 Wu 2003: 143.

obligations to assist in cybersecurity efforts, comply with data localization requirements, and cooperate with government agencies in law enforcement matters.[329]

4.3 CONTEMPORARY THEMES

The contemporary structure for regulating ISPs gives rise to certain contentious concepts and themes – some extrinsic and some intrinsic - which are central to this research. These are discussed below before the researcher moves to problematise the role and liability of ISPs against these factors.

4.3.1 INTERNATIONAL OBLIGATIONS

International obligations and intrinsic national policies profoundly influence China's contemporary regulatory structure of ISPs. This section explores how these external and internal factors shape the complex role and liability of ISPs within the Chinese digital landscape. China's engagement in global internet governance forums significantly impacts its domestic ISP regulations. China balances its national internet policy with global digital norms and practices as a key player in international platforms like the ITU and the WSIS. This participation allows China to influence and adapt to international standards, ensuring its ISPs operate within a globally interconnected framework.

However, China's approach to internet governance often contrasts with Western models, particularly regarding information control and censorship. While adhering to specific international standards, Chinese ISPs are also subject to domestic regulations prioritising state security and social stability.[330] This dual commitment presents a unique challenge for Chinese ISPs, who must navigate global internet norms and stringent national policies.

Cybersecurity has emerged as a critical area of focus in international internet governance in recent years. China's Cybersecurity Law, enacted in 2017, reflects a

[329] Yoo 2006: 1847.
[330] Yoo 2006: 1848.

concerted effort to align with global cybersecurity norms while asserting its concept of cyber sovereignty. This law imposes significant responsibilities on ISPs for data protection and mandates compliance with national security protocols.

Data sovereignty, integral to China's cybersecurity strategy, emphasizes the state's right to govern digital data within its territory. This approach impacts how Chinese ISPs manage data flows, requiring them to store certain data within national borders and comply with government requests for data access.[331] These requirements are often at odds with international principles advocating for the free flow of information,[332] posing a complex challenge for ISPs operating in the global digital economy. Intellectual property rights (IPR) are another critical aspect of China's international obligations impacting ISPs. China has reformed its IPR laws to protect intellectual property in the digital realm as part of its commitments to the WTO and under various bilateral trade agreements. ISPs in China are required to enforce these IPR standards, which involve monitoring and preventing the distribution of pirated or counterfeit digital content.[333]

China's participation in international trade agreements also influences its ISP regulations, especially concerning cross-border digital trade and e-commerce. ISPs play a crucial role in facilitating international e-commerce transactions, adhering to both domestic regulations and international trade protocols. This dual compliance ensures that Chinese ISPs support China's growing digital economy while respecting global trade norms.

While China's commitments to international human rights treaties, such as the ICCPR, should theoretically impact its ISP regulations, the reality is more complex. The Chinese government's stance on internet freedom and human rights often diverges from international standards. This divergence is evident in the restrictive measures imposed on ISPs regarding content censorship and surveillance.

331 Yoo 2006: 1849.
332 Yoo 2005: 3.
333 Wu 2003: 142.

Chinese ISPs must comply with domestic laws that limit freedom of expression and access to information on the internet. The state justifies these restrictions on grounds of national security and public morality, but they are often criticized internationally for violating basic human rights principles.[334] The role of ISPs in implementing these restrictive measures places them at the centre of a contentious debate between national policies and international human rights standards.

International obligations and national policies significantly shape the role and liability of ISPs in China. The balance between adhering to global internet governance norms and enforcing stringent domestic regulations presents a unique regulatory landscape for Chinese ISPs. As China continues to assert its position in the global digital arena, how its ISPs navigate these international and domestic obligations will be crucial in shaping the country's digital future. The tension between worldwide connectivity and national control remains a defining characteristic of China's approach to internet regulation, with ISPs playing a pivotal role in this dynamic interplay.

4.3.2 CONSTITUTIONAL FRAMEWORK

Understanding China's approach to ISPs necessitates an examination of its constitutional framework, fundamentally shaping the nation's Internet regulatory environment. Unlike many Western countries which explicitly safeguard freedom of expression and privacy, China's constitutional context reflects a different set of priorities and values that significantly influence the operations and liabilities of ISPs.

While proclaiming certain fundamental rights, China's constitution strongly emphasises state sovereignty and social stability. This emphasis has profound implications for ISPs operating within China. The state exerts considerable influence over the internet, viewing it as a crucial tool for economic development, national security, and societal harmony. Consequently, the constitutional framework allows for, and even mandates, a level of

[334] Yoo 2005: 3.

state control over digital communication that would be considered excessive in many other jurisdictions.

Under its constitutional prerogative, the Chinese government has enacted various laws and regulations directly impacting ISPs. These laws often prioritize national security and public morality over individual freedoms typically associated with internet usage. For instance, the Great Firewall of China – the colloquial name for China's internet censorship system – is a direct product of this constitutional prioritization. ISPs must comply with stringent censorship and surveillance laws, filtering content deemed inappropriate or harmful to national interests.[335]

Moreover, the Chinese Constitution provides a legal basis for the state's pervasive control over information dissemination. ISPs are expected to comply with censorship directives and are often enlisted to monitor and report on potentially subversive activities actively. This role extends beyond mere compliance, placing ISPs at the forefront of enforcing state policies on information control.

The constitutionally sanctioned priority of collective welfare over individual rights has led to a unique regulatory approach towards ISPs. While ISPs are seen primarily as commercial entities in many countries, in China, they are also viewed as partners in governance, instrumental in maintaining social order and advancing state policies. This perspective is evident in the Cybersecurity Law of 2017, which entrusts ISPs with significant responsibilities for data security and mandates cooperation with state surveillance efforts.

Additionally, China's approach to internet regulation reflects its broader governance style, marked by a top-down control mechanism. The state's directive on a harmonious society, deeply rooted in its constitutional ethos, is mirrored in its approach to internet governance.[336] ISPs, therefore, operate in an environment where adherence to state

335 Yoo 2005: 3.
336 Hu 2011: 526.

directives is not just a legal requirement but also a normative expectation aligned with the broader objectives of national harmony and stability.

The constitutional framework also influences the legal repercussions for ISPs that fail to comply with state regulations. Penalties for non-compliance can be severe, including hefty fines, revocation of licenses, and, in extreme cases, criminal charges.[337] This strict enforcement regime underscores the severe nature of ISP obligations under Chinese law.

However, this constitutional arrangement does not preclude all digital innovation and freedoms. The Chinese government recognizes the importance of the Internet in economic development and global competitiveness. As a result, while ISPs are tightly regulated in content and security, they are also encouraged and sometimes subsidized to advance in areas like broadband infrastructure development, 5G technology, and cloud computing.[338]

4.3.3 LEGISLATIVE FRAMEWORK

China's legislative framework for ISPs is sophisticated and multifaceted, reflecting the country’s unique approach to Internet regulation. The framework, built upon a complex array of laws and regulations, establishes the operational boundaries and responsibilities of ISPs within the Chinese digital ecosystem.

Central to this legislative structure is the Cybersecurity Law, enacted in 2017, which is the cornerstone of China’s internet regulation. This comprehensive law outlines a wide range of duties for ISPs, emphasizing cybersecurity, data protection, and user privacy. ISPs must implement robust measures to safeguard network security, prevent cyber-attacks, and report cybersecurity incidents to relevant authorities. This law underscores the critical role of ISPs in maintaining national cybersecurity and protecting digital assets.

337 Hu 2011: 526.
338 Hu 2011: 526.

Additionally, the Cybersecurity Law mandates real-name registration for users, placing the onus on ISPs to verify the identities of their subscribers.[339] This requirement is part of a broader strategy to control online anonymity and curb the spread of illegal content. ISPs are responsible for ensuring that their services are not used for activities that endanger national security, disrupt social order, or infringe upon the rights of others.

Another significant legislation is the Telecommunications Regulations of the People's Republic of China. This regulation provides the legal framework for telecommunications services, including those offered by ISPs. It stipulates licensing requirements, service standards, and the responsibilities of ISPs in providing fair and equitable services to the public.[340] The regulations also empower the government to manage and allocate internet resources, such as IP addresses and domain names, further tightening state control over the digital sphere.

The Great Firewall of China,[341] a central element of China's internet governance, though not a legislative document per se, is a manifestation of various legal directives that mandate ISPs to censor and block access to content deemed inappropriate or harmful by the state. This includes politically sensitive information, certain foreign websites, and content that violates public morality. The Firewall represents the legislative intent of controlling the digital information flow within China's borders, reinforcing the state's authority over digital content.[342]

Data protection is another critical aspect of the legislative framework. Personal Information Protection Law, complementary to the Cybersecurity Law, sets stringent data collection, processing, and storage guidelines. These laws place significant responsibilities on ISPs to protect user data from unauthorized access, disclosure, or

339 Hu 2011: 526.
340 Hu 2011: 528.
341 Stanford Edu "Free speech vs Maintaining social cohesion: a closer look at different perspectives" https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/FreeExpressionVsSocialCohesion/china_policy.html (Date of use: 12 December 2022).
342 Stanford Edu "Free speech vs Maintaining social cohesion: a closer look at different perspectives" https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/FreeExpressionVsSocialCohesion/china_policy.html (Date of use: 12 December 2022).

misuse. Compliance with these data protection laws is crucial for ISPs, especially in an era where data breaches can have far-reaching consequences.[343]

China's legislative approach to online content and information dissemination is also reflected in laws such as the Provisions on the Governance of the Online Information Content Ecosystem. These provisions categorize online content into 'positive' and 'negative' content, guiding ISPs on content moderation. ISPs must promote content that upholds socialism's core values while suppressing content considered false, harmful, or violating public order.[344]

Moreover, China's approach to international digital cooperation is governed by its participation in various international treaties and agreements. ISPs must comply with these international commitments while adhering to domestic laws, which requires careful navigation of global and local regulatory landscapes. In addition to these laws, various administrative regulations and guidelines issued by regulatory bodies like the Ministry of Industry and Information Technology (MIIT) and the Cyberspace Administration of China (CAC) provide detailed operational guidelines for ISPs.[345] These regulations cover aspects ranging from service provision standards to emergency response protocols for cybersecurity incidents.

4.3.4 JUDICIAL INTERPRETATION

Judicial interpretation plays a crucial role in shaping the operational landscape of ISPs in China. How Chinese courts interpret and apply laws relevant to ISPs has profound implications for their practices, particularly in a regulatory environment as complex and multifaceted as China's. A significant aspect of judicial interpretation concerns the Cybersecurity Law. Chinese courts have often been called upon to interpret various provisions of this law, especially those relating to data protection, privacy, and national

343 Greenleaf 2021: 23.
344 Dongjin Consulting "Provisions on Governance of the Network Information Content" http://en.shanghaiinvest.com/information-center/newsletters/item/333-provisions-on-governance-of-the-network-information-content (Date of use: 12 April 2020).
345 Hu 2011: 528.

security. These interpretations provide crucial guidance for ISPs on compliance with cybersecurity standards and data processing norms. For instance, judicial decisions on what constitutes “critical information infrastructure” directly affect the security measures and compliance obligations of ISPs.

Judicial interpretation also extends to content regulation and censorship, central to ISP operations in China. Courts have elaborated on ISPs' responsibilities for monitoring and censoring content, clarifying the extent of liability in cases of failure to remove prohibited content. These interpretations often involve a delicate balance between enforcing state censorship policies and respecting the operational autonomy of ISPs.[346] One notable area is the interpretation of laws concerning the “Great Firewall”.[347] While the Firewall itself is not a judicial creation, court rulings on cases involving bypassing or violating state-imposed internet censorship provide legal backing to this massive digital censorship apparatus.[348] ISPs, guided by these rulings, implement measures to block or filter content in line with state directives, understanding the legal consequences of non-compliance.

With the increasing importance of data in the digital economy, Chinese courts have also interpreted laws relating to data privacy and protection. Judicial decisions in this area influence how ISPs collect, store, and use customer data. These interpretations help ISPs navigate the complexities of complying with China’s stringent data protection regime, ensuring they do not inadvertently breach privacy laws while handling vast amounts of user data. Judicial interpretation in the realm of cybercrime is another critical area for ISPs. The courts have defined various aspects of cybercrime, including unauthorized data access, cyber fraud, and online intellectual property infringement.

346 Wu 2003: 148.
347 Stanford Edu “Free speech vs Maintaining social cohesion: a closer look at different perspectives” https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/FreeExpressionVsSocialCohesion/china_policy.html (Date of use: 12 December 2022).
348 Wu 2003: 149.

These definitions and legal precedents inform ISPs' internal policies on user conduct and cooperation with law enforcement agencies in cybercrime investigations.[349]

Chinese courts often resolve ambiguities in the legislative framework affecting ISPs. In a rapidly evolving digital landscape, new technologies and business models may create scenarios not explicitly covered by existing laws. Judicial interpretations in these instances provide much-needed clarity, helping ISPs align their operations with legal expectations. Although Chinese courts primarily focus on domestic laws, their interpretations occasionally consider international legal principles, especially in cases involving cross-border data flows and international cooperation.[350] These interpretations help ISPs understand their obligations in the context of China's international commitments and global internet governance standards.

4.4 INTERNET SERVICE PROVIDERS – PRESENT CHALLENGES AND LEGISLATIVE RESPONSE

4.4.1 INTERNET SERVICE PROVIDER LIABILITY IN THE PEOPLE'S REPUBLIC OF CHINA

China establishes the liability of ISPs through internet censorship programs that seek to give ISPs and other intermediaries the duty to monitor, filter, and censor the data transmitted through their websites, servers, and networks. This system of censorship manifests in two ways. Firstly, it manifests through a complex system of regulations that give intermediaries the power to monitor the activities of Internet users. Secondly, the country's censorship manifests through the technologies that the Chinese government uses to acquire information from internet users and utilises that information to punish individuals violating the country's laws.

349 Sorbán 2019: 23.
350 Wu 2003: 149.

4.4.2 INTERNET LAWS AND REGULATIONS IN THE PEOPLE'S REPUBLIC OF CHINA

Unlike the USA and the EU, China uses a proactive approach to the determination of ISPs' liability. The country uses a "guilty until proven innocent" approach to determine the liability of ISPs and other intermediaries.[351]

Under the "Great Firewall of China," the country has developed a complex system of human oversight policies, technologies, and laws that control all aspects of the web content that internet users transmit, store, view, and share. Scholars argue that China's complex liability system has confounded many critics who say it was impossible with the rapid expansion of the internet.[352]

The Chinese government marked the first step in its quest to restrict access to the Internet in 1996 when it enacted the Interim Provisions Governing Management of Computer Information Networks in the People's Republic of China Connecting to the International Network (PGMC). Between 1998 and 2000, the Chinese government strengthened the PGMC by amending it.

The government amended it by enacting the State Council Order 292 and the Provisions for implementing the Interim Provisions Governing the Management of Computer Information Networks in the People's Republic of China.

The country amended the principal law in the same period by enacting the Decision of the Standing Committee of the National People's Congress on Preserving Computer Network Security[353] and Measures on Internet Information Services.[354] The original

---

351 Greenleaf 2021: 23.
352 Greenleaf 2021: 23.
353 "Decision of the Standing Committee of the National People's Congress on Preserving Computer Network Security" http://english.gov.cn/laws/2005–09/22/content_68771.htm.(Date of use: 10 December 2016).
354 "Measures on Internet Information Services" http://www.transasialawyers.com/translation/legis_16_e.pdf (Date of use: 10 December 2016).

provisions and the provisions introduced into the principal law by virtue of the amendment have imposed complete censorship on internet content.[355]

Internet regulations make it unlawful for intermediaries to display content without the express approval or authorisation of the Chinese government.[356] The laws list the type of data ISPs and other intermediaries cannot display without the government's express approval. This data includes information on violence, gambling, pornography, obscenity, and feudal superstitions.[357]

Other categories of information that the ISPs and other intermediaries cannot display include information that might lead to the disruption of the public order, information that might lead to the disruption of the social order, information regarded as State secrets, information that might subvert the Chinese government, and information that tends to contradict, or ignore, the government's policy on religion.[358]

These provisions suggest that the Chinese government has structured its internet censorship laws in a way that is so wide that it covers all the activities of intermediaries. The broad scope confirms that the government has opted against the American approach of allowing intermediaries to identify and delete the infringing content.

In China, the mere presence of infringing material on the website, network, or intermediaries' servers proves that the intermediary has violated the country's laws. Furthermore, evidence of the extent of the country's censorship and its strict application

355 Flyverbom et al. 2019: 17.

356 "Decision of the Standing Committee of the National People's Congress on Preserving Computer Network Security" http://english.gov.cn/laws/2005–09/22/content_68771.htm.(Date of use: 10 December 2016).

357 "Decision of the Standing Committee of the National People's Congress on Preserving Computer Network Security" http://english.gov.cn/laws/2005–09/22/content_68771.htm.(Date of use: 10 December 2016).

358 "Decision of the Standing Committee of the National People's Congress on Preserving Computer Network Security" http://english.gov.cn/laws/2005–09/22/content_68771.htm.(Date of use: 10 December 2016).

of third-party liability laws stems from the provisions on the responsibility of intermediaries concerning the handling of content that violates the country's laws.

In addition to the identified rules, the principal legislation states that intermediaries specialising in transmitting information services must seek a commercial or private license.[359] The commercial- and private licenses impose further rules that require the intermediaries to monitor and filter the activities of internet users.[360]

These licenses state that an intermediary will only obtain it by recording the domain name, IP address, and other categories of information necessary for identifying the internet users using their news websites, servers, and networks to share information with their target audiences.[361] Furthermore, the laws state that the ISPs must record and retain this information for 60 days.[362]

The ISPs must also record the internet users' dial-up numbers, IP addresses, bank account details, and hours they spend online.[363] When the intermediaries discover incriminating content while assessing the internet users' data, they must block it, record it, and communicate it with the relevant authorities.[364]

These provisions show the extent of the country's responsibility to the ISPs and other intermediaries. The nature of the obligation imposed on the intermediaries suggests that the country cannot license an intermediary if it does not have the technological infrastructure needed to monitor, block, record, and report internet users or content violating the country's laws.

The structure of the laws suggests that the country's government will only open the country's doors to intermediaries that show that they possess the technology needed to

359 Measures on Internet Information Services, Article 55.
360 Measures on Internet Information Services, Article 55.
361 Measures on Internet Information Services, Article 14.
362 Measures on Internet Information Services, Article 14.
363 Measures on Internet Information Services, Article 14.
364 Measures on Internet Information Services, Article 14.

comply with existing laws. Where the evidence shows that an intermediary cannot comply with the country's laws, the government will deregister the intermediary or cancel its license application. Deregistration of the intermediary and cancellation of the intermediary's license forces them to choose between losing earnings and compliance with the country's laws. Failing to comply with the country's laws means the government will lock the intermediaries out of the country's lucrative market.

Complying with the country's laws will create the impression that the intermediaries are prioritising the profits at the expense of the rights of the country's citizens. This is a dilemma that intermediaries like Google and Yahoo have faced, and they continue to show to the outside world that they will prioritise profits at the expense of the rights of citizens in China and Taiwan.

In 2005, the Chinese government underlined its willingness to strengthen its strict online censorship laws when it enacted new regulations to govern intermediaries specialising in transmitting "*Internet news*".[365] The new regulations defined this new category of intermediaries as those specialising in transmitting news on political and current affairs, including reports on social and public affairs like sudden events and diplomatic, military, economic, and political events and affairs.

The new law stipulates that an intermediary will fall into the new category of intermediaries, even if it only provides an online bulletin board for internet users to comment.[366] The law contains all the content restrictions of the previous laws, but it has added a provision limiting those intermediaries to information released by the government's news agencies.

The new requirement means that the law prevents intermediaries like Facebook, Twitter, and Weibo from publishing information and other categories of content emanating from bloggers and journalists. Although the law does not expressly state that the

365 Greenleaf 2021: 23.
366 Wu 2003: 148.

intermediaries cannot post information from bloggers, it states that they can only publish approved information.

This approved information restricts the intermediaries to information published by the Chinese government. It means that the intermediaries cannot transmit information from bloggers and other citizen journalists without the express approval of the Chinese government. The other implication of the law is that the intermediaries must “dumb down” their content by limiting themselves to gossip. This move has transformed reputable blogging websites into tabloid columns that do not add value to Chinese society.

Apart from complying with the 2005 law, the intermediaries classified as Internet news intermediaries must comply with the provisions of the Administration of Internet Electronic Messaging of 2000. This law requires all intermediaries operating online bulletin boards to seek the approval of the Chinese government before they begin to undertake such operations.

As a part of the efforts to comply, the law states that such organisations must display their permit number on their online bulletin boards, outline the code of conduct that subscribers must respect, and warn subscribers about the legal consequences that might visit them if they violate the code of conduct.

The law also states that a company with bulletin board services must implement censors to ensure that the content in chat rooms and the boards comply with the government’s restrictions on communication content. The essence of this provision is that it restricts not only the services of the bulletin board intermediaries but also the services of the social media networks.

Bulletin board intermediaries and social media intermediaries supply similar services. In bulletin boards, subscribers can communicate directly with other public members or restrict people from seeing their communications by opening private chat rooms.

Similarly, Facebook- and Twitter users can communicate with the public by posting messages on their timelines or restricting information using direct messaging services.

Filters prevent users from using chat rooms and direct messaging services to send messages or exchange information that violates the country's laws. The censor technologies will block and record the information so the intermediary can inform the government about the infringement.

The technologies aim to ensure that the intermediaries know the identity of all the individuals and organisations transmitting data through their networks, servers, and websites. The intermediaries providing bulletin boards, social networking services, and other services that allow users to communicate publicly[367] and in chat rooms must know the identity of all the users accessing their services.

Subscribers cannot use email addresses, usernames, and other data that conceal their identity. They must furnish all the documents relating to their identity. The elimination of software technologies that anonymise users makes it easier for the government to search for and arrest online users in instances where their actions have contributed to violating the country's laws. In such cases, the intermediaries become the conduits that the Chinese government uses to identify and arrest the individuals who have broken the law.[368]

Even with the existing strict legal rules, the Chinese government has enacted another law giving ordinary citizens the power to identify and report people engaging in creating or disseminating data that subverts the government or violates the country's laws. The Chinese government allows citizens to report violations via the Public Pledge of Self-Regulation and Professional Ethics for China's Internet Industry.[369]

---

367 Internet Society of China "Introduction" https://www.isc.org.cn/en (Date of use: 16 December 2017).

368 Internet Society of China "Introduction" https://www.isc.org.cn/en (Date of use: 16 December 2017).

369 Internet Society of China "Introduction" https://www.isc.org.cn/en (Date of use: 16 December 2017).

This law allows citizens to report websites and other online intermediaries suspected of creating and transmitting content that might violate the country's laws.

The law's definition of citizens is broad enough to cover ordinary citizens and all companies registered in China. The law states that all citizens and companies must ensure that the information published, transmitted, or stored on servers, websites, or networks does not violate the country's laws.[370]

The law adds that citizens and companies must delete all information harmful to the country and its government. It adds that this duty extends to deleting links to websites and networks that might contain harmful data.[371] To enhance the speed of reporting, the law states that the government will establish a website where citizens can report websites or companies violating the country's laws by publishing harmful content.[372]

The existing evidence suggests that the government has already established this website and has used evidence that citizens have posted to arrest and incarcerate individuals who spread malicious information.

4.4.3 TECHNOLOGICAL MEASURES IMPLEMENTED TO ENHANCE THE LIABILITY OF INTERMEDIARIES IN THE PEOPLE'S REPUBLIC OF CHINA

To back up the extensive system of laws and intensify the liability of intermediaries, the Chinese government has implemented an elaborate technological network that can detect and filter out content even before it reaches the networks, serves, and websites belonging to the intermediaries. The Chinese government refers to its censorship infrastructure as the Chinese Internet System (CIS).[373] The CIS has two layers of censorship designed to stop intermediaries from transmitting, storing, and processing

370 Internet Society of China "Introduction" https://www.isc.org.cn/en (Date of use: 16 December 2017).
371 Measures on Internet Information Services, Article 9.
372 Measures on Internet Information Services, Article 9.
373 Internet Society of China "Introduction" https://www.isc.org.cn/en (Date of use: 24 December 2022).

data that has content that will undermine or violate the country's laws and the legitimacy of the country's leadership.[374]

The first layer consists of the network segment that is visible and accessible to the public. ISPs and other intermediaries can connect to this layer to provide services to their target market in China. The technological infrastructure of the first layer is so robust that the intermediaries operating in China cannot provide their services without connecting to it.[375]

The first layer of internet technology permits citizens to access online content created and transmitted in the country. When intermediaries want to help users access the content created outside the country, they can only do so through the second layer.[376]

The second layer is invisible to the public and is under the complete control of the Chinese government. The Chinese government polices the boundaries that separate the CIS from content published outside the country. The strength of the second layer has led scholars to refer to it as China's intranet. The backbone of the second layer consists of advanced and powerful network and censorship technologies.[377]

From 2004 to 2005, the OpenNet Initiative [378] conducted a study on the effectiveness of the network in censoring content created and transmitted outside the country and discovered that it uses sophisticated Cisco routers to give it these dynamic filtering capabilities. The dynamism of the filtering measures has permitted the company to develop 750,000 filtering rules that can identify and block malicious data before it gets to the country. The OpenNet study also revealed that the backbone of the second tier

374 Wu 2003: 155.
375 Internet Society of China "Introduction" https://www.isc.org.cn/en (Date of use: 24 December 2022).
376 Internet Society of China "Introduction" https://www.isc.org.cn/en (Date of use: 24 December 2022).
377 Greenleaf 2021: 29.
378 OpenNet Initiative "Country Profile: China" https://opennet.net/countries/china (Date of use: 12 December 2023).

has sophisticated network security software and a firewall that can identify and block certain types of data from reaching consumers in the country.[379]

The complex censorship technology has been helpful to the intermediaries by preventing them from accessing content that might violate the law. The censorship system blocks the information and prevents it from reaching the target audience in China. During its study, researchers at OpenNet attempted to infiltrate the country's internet by sending messages, emails, and other categories of data to addresses and websites in China.

The results show that some of the information reached the target audience while the rest did not reach the targeted audience. The study shows that the information on Taiwan independence, Tibetan Independence, Falun Gong, and the Tiananmen Square massacre could not breach the firewall and reach its intended destination.[380]

The study shows that the targeted user could not access the content from China. The results showed that the complex security system intercepted some of the emails containing information on the Tiananmen Square massacre, Falun Gong, Taiwan Independence, Tibetan Independence, and the other categories of data that the State considers sensitive. However, the data suggests that the internet system in China is defective, as certain messages go through the complex network.

The researchers discovered they could still send messages on Tibetan Independence, Tiananmen Massacre, Falun Gong, and Taiwan Independence by changing the sensitive data's wording, language, or character. Changing the language and characters of the encoding message made it easier for the sensitive data to sail through to its intended target.

The researchers also discovered that the censoring technology was not mature enough to detect infringing content sent privately through online chat rooms. However, the

379 OpenNet Initiative "Country Profile: China" https://opennet.net/countries/china (Date of use: 12 December 2023).

380 OpenNet Initiative "Country Profile: China" https://opennet.net/countries/china (Date of use: 12 December 2023).

censorship system excluded websites with sensitive information from search results.[381] The exclusion of websites means that ordinary Chinese citizens cannot access all data the government categorises as sensitive.

Nonetheless, it is important to note that the Chinese government could not have achieved this significant success without the assistance of corporations in the USA. The Chinese government and private sector cannot initiate nationwide filtering and censorship campaigns. The success of the government's filtering and censorship campaigns hinges heavily on the support from American companies like Cisco Systems, Sun Microsystems, and Websense.[382]

Cisco Systems provides sophisticated routers that enable the Chinese government to define up to 750,000 filtering rules. Websense and Sun Microsystem provide the Chinese government with the hardware and software to assist it in conducting a nationwide monitoring campaign. The two companies have also assisted the Chinese government in developing sophisticated filtering technologies that prevent internet users in China from accessing information that violates the country's laws.

The support offered to the Chinese government by the American companies is surprising, especially considering how many of these companies pride themselves in respect for the rule of law and human rights. Many of these Western companies are aware that the Chinese government use their technologies to arrest, detain, and even kill internet users, but they continue to provide these services.

One factor that leads them to continue providing these services is the money they receive from the Chinese government.[383]

---

381 OpenNet Initiative "Country Profile: China" https://opennet.net/countries/china (Date of use: 12 December 2023).

382 OpenNet Initiative "Country Profile: China" https://opennet.net/countries/china (Date of use: 12 December 2023).

383 At the time of writing litigation was underway in the USA to block continued sale of Cisco Servers in China.

4.4.4 THE SUCCESS OF THE CHINESE GOVERNMENT

China's investment in its legal infrastructure and the technology to support legal censorship leads many to wonder whether the government has succeeded in its quest to censor intermediaries and hold them liable for violating the country's laws. An analysis of data from the government suggests that the government has successfully held intermediaries to account. In particular, the available data indicates that the country has managed to hold the Western intermediaries, like Google and Yahoo, to account.

The relationship between the Chinese government and Yahoo offers insight into the country's success in holding the intermediaries to account. Immediately after the Chinese government enacted censorship laws, the Chinese government and Yahoo entered into an agreement called the Public Pledge on Self-discipline for the Chinese Internet Industry.[384] As a part of the agreement, Yahoo underlined its commitment to implement systems that would make it easier to filter and block content infringing on Chinese laws.

Further, the internet giant stated that it would refrain from providing links that redirect internet users to websites with harmful content to the country's government and its citizens. Yahoo stated that its decision to agree was voluntary, and it did not believe that the strict regulation compelled it to enter into such agreements.[385]

After signing this agreement, an attempt to use the Yahoo search engine to seek sensitive information returned negative results. In 2005, international media companies highlighted the extent of Yahoo's collaboration with the Chinese government when they revealed the role that Yahoo has played in the arrest of a human rights activist in China.

---

384 The Guardian "Chinese sites agree to censor content" https://www.theguardian.com/technology/2002/jul/16/onlinesecurity.internetnews (Date of use: 13 December 2022).

385 The Guardian "Chinese sites agree to censor content" https://www.theguardian.com/technology/2002/jul/16/onlinesecurity.internetnews (Date of use: 13 December 2022).

The media stated that Yahoo contributed to the arrest of the activist by giving the government the IP address, which enabled it to identify the address of the human rights activist. Yahoo defended its action by claiming it decided to share the IP address because the Chinese government informed it that the activist was leaking State secrets.[386]

However, the international media suggests that the alleged "State secret" was information about the actions which the Chinese government had implemented to prevent the country's citizens from celebrating the 15th anniversary of the Tiananmen Square massacre. After the arrest, a Chinese Court sentenced the activist to a prison term of ten years for the crime of leaking State secrets.[387]

Such an outcome led to the widespread condemnation of Yahoo's actions. Many people argued that Yahoo was responsible for the arrest of the activist.[388] China's ability to arrest the human rights activist and Yahoo's role in his arrest showed that the country's laws successfully enabled the government to hold intermediaries to account.

However, Yahoo is not the only company from the West that the Chinese government has held to account. In 2002, Google announced that it was developing a new search engine to target users in China. The company announced that the new search engine

386 Guo "Inside the decades-long fight over Yahoo's misdeeds in China" https://www.technologyreview.com/2023/12/12/1084990/yahoo-china-dissident-yahoo-human-rights-fund/#:~:text=In%202002%2C%20Yahoo%2C%20whose%20CEO,end%20of%20one%2Dparty%20rule. (Date of use: 9 January 2024).

387 Guo "Inside the decades-long fight over Yahoo's misdeeds in China" https://www.technologyreview.com/2023/12/12/1084990/yahoo-china-dissident-yahoo-human-rights-fund/#:~:text=In%202002%2C%20Yahoo%2C%20whose%20CEO,end%20of%20one%2Dparty%20rule. (Date of use: 9 January 2024).

388 Guo "Inside the decades-long fight over Yahoo's misdeeds in China" https://www.technologyreview.com/2023/12/12/1084990/yahoo-china-dissident-yahoo-human-rights-fund/#:~:text=In%202002%2C%20Yahoo%2C%20whose%20CEO,end%20of%20one%2Dparty%20rule. (Date of use: 9 January 2024).

would have none of the features available to users of the Google search engine in other parts of the world.[389]

The company claimed that the search engine would not have services like Gmail and Google News, but it informed users worldwide that it would use its systems to resist attempts by the Chinese government to censor its activities.[390] However, the Chinese government reacted to this news by blocking *Google. Cn.* search engine in 2002. In 2004, Google approached the Chinese government and asked it to lift the ban on *Google.cn.*

The Chinese government said it would only lift the ban if Google agreed to abide by the country's censorship laws. In 2006, Google announced that it was launching its search engine in compliance with Chinese censorship laws. The search engine gave Chinese consumers access to a version of Google News that excluded links from websites and publications that the Chinese government categorized as objectionable.[391]

The Google News webpage allowed the users to access the websites and webpages the Chinese government had pre-approved. Google attempted to protect its public image by stating that it would inform internet users about the censored search results. It also attempted to save its image by announcing that it would exclude Gmail and Google blogs from the search because it did not want the Chinese government to force it to collect the personal information of individuals accessing its services.[392]

---

389 Gallagher "Google plans to launch censored search engine in China, leaked documents reveal" https://theintercept.com/2018/08/01/google-china-search-engine-censorship/ (Date of use: 12 December 2023).

390 Gallagher "Google plans to launch censored search engine in China, leaked documents reveal" https://theintercept.com/2018/08/01/google-china-search-engine-censorship/ (Date of use: 12 December 2023).

391 Gallagher "Google plans to launch censored search engine in China, leaked documents reveal" https://theintercept.com/2018/08/01/google-china-search-engine-censorship/ (Date of use: 12 December 2023).

392 Gallagher "Google plans to launch censored search engine in China, leaked documents reveal" https://theintercept.com/2018/08/01/google-china-search-engine-censorship/ (Date of use: 12 December 2023).

These attempts proved futile after data showed that the information blocked by the Google search engine was more significant than the information blocked by the Chinese and Yahoo search engines. This outcome proved that the Chinese government's attempts to hold the intermediaries to account were successful. The government has implemented a system that gives it the power to block the services of intermediaries that do not want to comply with the country's censorship laws.

The government blocked Google and forced it to choose between its profits and public image. In the end, Google decided to prioritise its profits at the expense of the rights of Chinese citizens. Like Google and Yahoo, Microsoft has acceded to the Chinese internet laws and decided to abide by the rules requiring the intermediaries to record information on the identities and IP addresses of all individuals and organisations using their network, websites, and servers to transmit information to other internet users.[393]

Microsoft's history of compliance with the censorship laws and rules in China is like that of Google. Microsoft began its activities in the country by stating that it would not comply with the country's laws on censorship and intermediary liability. The company indicated that implementing such rules would be akin to violating internet users' privacy and freedom of expression guarantees. Nonetheless, Microsoft's attempts to reject China's censorship laws failed after the Chinese government blocked the company's services.[394]

China implemented a rule stating that Microsoft could not establish its services in the country. Microsoft, however, changed its stance on censorship and agreed to comply with the censorship activities of the Chinese government. It agreed to remove offending blogs, images, and videos from its webpage. This change of stance led to the Chinese government's announcement in 2005 that it had lifted the ban on Microsoft's operations in China.[395]

---

393 Simonite "US Companies help censor the internet in China, too" https://www.wired.com/story/us-companies-help-censor-internet-china/ (Date of use: 12 January 2022).

394 Simonite "US Companies help censor the internet in China, too" https://www.wired.com/story/us-companies-help-censor-internet-china/ (Date of use: 12 January 2022).

395 Simonite "US Companies help censor the internet in China, too" https://www.wired.com/story/us-companies-help-censor-internet-china/ (Date of use: 12 January 2022).

Microsoft announced it would make its online blog services (MSN Spaces) available to subscribers. Still, it stated that it had implemented filters to prevent the users from uploading stories, videos, and images, violating the country's laws. Immediately after the launch of MSN Spaces, internet users in China began to report that they could not upload stories containing words like "democracy," "demonstration," "human rights," and "freedom."[396]

Attempts to upload documents with these words returned error messages stating that the Chinese government had classified one or more of the words in the content as "forbidden speech".[397] Microsoft compounded the situation in December of the same year (2005) when reports emerged that it had blocked and removed a blog by a government critic at the request of the country's government. The reports indicated that Microsoft had removed Michael Anti's blog after the Chinese government raised concerns about the content on his blog.[398]

4.5 PRELIMINARY CONCLUSION

As this chapter draws to a close, it becomes evident that the role and liability of ISPs in China are deeply intertwined with the country's unique socio-political fabric and its overarching state-centric approach to Internet governance. This conclusion aims to encapsulate the key insights gained from exploring China's ISP landscape and reflect on the implications and lessons that can be drawn for other contexts, particularly South Africa.

Firstly, China's historical journey with ISPs, characterized by a transition from state control to gradual liberalization, highlights the state's strategic role in shaping the internet landscape. This journey underlines the significant influence of political and economic

396 Simonite "US Companies help censor the internet in China, too" https://www.wired.com/story/us-companies-help-censor-internet-china/ (Date of use: 12 January 2022).
397 Simonite "US Companies help censor the internet in China, too" https://www.wired.com/story/us-companies-help-censor-internet-china/ (Date of use: 12 January 2022).
398 Simonite "US Companies help censor the internet in China, too" https://www.wired.com/story/us-companies-help-censor-internet-china/ (Date of use: 12 January 2022).

considerations in the evolution of ISP regulation. The Chinese model, where state interests heavily dictate the operational scope of ISPs, contrasts markedly with more liberal regulatory frameworks, offering a unique perspective on the diversity of global internet governance models.

As examined in this chapter, the contemporary regulatory environment in China reveals a complex interplay of international obligations, constitutional directives, legislative frameworks, and judicial interpretations. Chinese ISPs operate within a tightly controlled regime, balancing obligations to global internet norms with stringent domestic regulations. This balance, often skewed towards national control, raises critical questions about the extent to which ISPs can be independent entities in a state-dominated landscape.

The Chinese approach to internet governance, particularly its emphasis on content control and surveillance, underscores a broader debate about the limits of state authority in the digital realm. The stringent measures imposed on ISPs in China for content filtering and data protection highlight a governance model prioritising national security and public order over individual digital freedoms.[399] This approach starkly contrasts models prioritising individual rights, offering an essential perspective on the range of governance strategies in the digital age.

Moreover, the role of ISPs in China as enforcers of state policies has significant implications for the discourse on digital rights and freedoms. The Chinese case illustrates the challenges ISPs face in balancing their commercial interests with their role as implementers of state directives. This balance is particularly precarious in areas such as data privacy, where ISPs are caught between complying with government mandates and protecting user rights.

The insights from China's ISP landscape offer valuable lessons for other countries, including South Africa. China's model presents a cautionary tale of the potential pitfalls

[399] Dharmawan et al. 2019: 3177.

of excessive state control for nations grappling with the challenges of regulating the digital space. However, it also offers lessons in implementing robust cybersecurity measures and fostering technological innovation within a regulated framework.

CHAPTER FIVE

THE ROLE AND LIABILITY OF INTERNET SERVICE PROVIDERS IN IRELAND

5.1 INTRODUCTION

In this chapter, the researcher delves into the intricate world of ISPs in Ireland, a landscape characterized by its nuanced balance of regulatory frameworks, digital freedoms, and ISP liabilities. The objective is not merely to map out the operational terrain of Irish ISPs but also to draw meaningful comparisons with the South African context. This comparative analysis aims to unearth lessons and best practices that could potentially refine and enhance the South African ISP regulation and liability approach.

Ireland presents a fascinating case study with its unique position in the EU and as a hub for many global tech companies. The country's legal and regulatory framework for ISPs has evolved in the context of EU directives and national priorities, offering a rich tapestry of legal precedents, regulatory practices, and judicial interpretations. This chapter seeks to dissect these elements, analysing how Ireland navigates the complex interplay between internet governance, ISP liability, and user rights.

A pivotal aspect of this exploration is understanding the role and liability of ISPs in the broader context of Ireland's digital policy landscape. Irish ISPs operate in an environment where EU regulations and global digital trends exert a significant influence. This scenario presents a unique set of challenges and opportunities for ISPs, particularly in data protection, content regulation, and network neutrality.[400] The chapter will scrutinize these areas, focusing on how Irish ISPs balance their operational imperatives with legal and ethical responsibilities.

[400] Eloff 2020: 8.

Additionally, this chapter will delve into the specific legislative and policy frameworks that govern ISPs in Ireland. Central to this discussion will be the EU's GDPR, which has set a new data privacy and protection standards benchmark. The implementation of GDPR in Ireland and its implications for ISPs offer valuable insights into the evolving nature of data protection and the role of ISPs in safeguarding user privacy.

Another area of focus will be the judicial interpretation of laws and regulations affecting ISPs in Ireland. Irish courts have played a crucial role in shaping the legal landscape for ISPs, particularly in interpreting the balance between freedom of expression, right to information, and privacy. This judicial perspective is essential in understanding the operational realities and legal boundaries within which Irish ISPs function.

The comparative dimension of this chapter will highlight the contrasts and parallels between the Irish and South African approaches to ISP regulation. This comparison is instrumental in identifying potential lessons for South Africa, especially considering Ireland's success in creating a conducive environment for digital innovation while maintaining robust regulatory standards. The researcher will explore whether and how South Africa can draw from Ireland's experiences to refine its regulatory framework, particularly in fostering a competitive ISP market that upholds user rights and adheres to international best practices.

In addition to regulatory and legal aspects, this chapter also considers the socio-economic and cultural factors that influence ISP operations in Ireland. Ireland's unique position as a technologically advanced nation with deep cultural roots provides a broader context for understanding the role of ISPs in society. The chapter examines how ISPs contribute to Ireland's digital economy, their challenges in an increasingly interconnected world, and the societal implications of their operations. Lastly, the chapter aims to contribute to the broader body of knowledge on internet governance and ISP liability. By comprehensively analysing the Irish model, the researcher seeks to inform action, enrich academic discourse, and offer practical insights that could be instrumental in shaping policy and regulatory frameworks in South Africa and beyond. This contribution is

academic and pragmatic, aimed at influencing policy decisions and legal reforms in Internet governance's dynamic and ever-evolving domain.

5.2 INTERNET SERVICE PROVIDERS – HISTORICAL DEVELOPMENT

The evolution of ISPs in Ireland is a compelling narrative that mirrors the country's journey towards becoming a digitally advanced society. This section delves into the historical development of ISPs in Ireland, tracing their origins, growth, and transformative role in shaping Ireland's digital landscape.

The history of ISPs in Ireland begins in the late 1980s and early 1990s, a period marked by the nascent stages of the internet.[401] The initial phase was predominantly characterized by academic and research institutions laying the groundwork for internet connectivity. The pioneering ISPs during this era were typically small-scale operations, offering dial-up services that gave the public their first taste of the internet.[402] This period was crucial in setting the stage for a broader internet adoption, driven by a growing recognition of its potential to revolutionize communication and information access.

The mid to late 1990s witnessed a significant expansion and commercialization of ISP services in Ireland.[403] This era saw the emergence of more ISPs, spurred by the deregulation of the telecommunications sector and the Irish government's commitment to fostering a knowledge-based economy.[404] The competition among ISPs led to improved services and more affordable internet access for consumers and businesses alike. This period was pivotal in democratizing internet access, laying the foundation for the digital society that Ireland aspired to become.

---

401 TechArchives "How the internet came to Ireland" https://techarchives.irish/how-the-internet-came-to-ireland-1987-97/ (Date of use: 13 January 2022).

402 TechArchives "How the internet came to Ireland" https://techarchives.irish/how-the-internet-came-to-ireland-1987-97/ (Date of use: 13 January 2022).

403 Murphy "History of the Irish Internet" http://www.internethistory.ie/ (Date of use: 13 January 2022).

404 TechArchives "How the internet came to Ireland" https://techarchives.irish/how-the-internet-came-to-ireland-1987-97/ (Date of use: 13 January 2022).

The early 2000s marked the beginning of the broadband revolution in Ireland. ISPs began transitioning from dial-up to broadband services, offering faster internet speeds and more reliable connections.[405] This shift was a game-changer, facilitating the emergence of a digital economy and enabling the proliferation of online services. However, this period also saw market consolidation, with larger ISPs acquiring smaller ones, leading to a more concentrated market. This consolidation was driven by the need for significant investments in infrastructure to support broadband services, which smaller ISPs often found challenging to muster.[406]

Throughout this historical development, regulatory frameworks played a crucial role. Through agencies like the Commission for Communications Regulation (ComReg), the Irish government implemented policies and regulations that shaped the ISP market.[407] These included licensing requirements, consumer protection measures, and rules governing competition among ISPs. The regulatory environment was instrumental in ensuring a level playing field, promoting innovation, and safeguarding consumer interests.

Advancements in technology have continually influenced the development of ISPs in Ireland. The introduction of fibre-optic technology and the rollout of high-speed broadband networks marked the latest phase of this evolution.[408] These technological advancements have enabled ISPs to offer services beyond internet connectivity, including digital television, VoIP, and cloud computing solutions. This diversification has been critical in keeping Irish ISPs competitive and relevant in a rapidly evolving global digital market.

ISPs have been central to the growth of Ireland's digital economy. They have facilitated e-commerce, online education, remote working, and other digital services that have

405 Murphy "History of the Irish Internet" http://www.internethistory.ie/ (Date of use: 13 January 2022).
406 Murphy "History of the Irish Internet" http://www.internethistory.ie/ (Date of use: 13 January 2022).
407 TechArchives "How the internet came to Ireland" https://techarchives.irish/how-the-internet-came-to-ireland-1987-97/ (Date of use: 13 January 2022).
408 TechArchives "How the internet came to Ireland" https://techarchives.irish/how-the-internet-came-to-ireland-1987-97/ (Date of use: 13 January 2022).

become integral to modern life. The development of data centres by major ISPs has also positioned Ireland as a key player in the global digital economy, attracting multinational corporations to set up their European headquarters.[409]

Despite the successes, ISPs in Ireland face contemporary challenges, including bridging the digital divide, ensuring data privacy and security, and navigating complex EU regulations like GDPR. The prospects for ISPs in Ireland hinge on their ability to address these challenges while continuing to innovate and expand their services. The ongoing rollout of 5G technology and the increasing demand for Internet of Things (IoT) connectivity present new opportunities for growth and innovation.

5.3 CONTEMPORARY THEMES

The contemporary structure for regulating ISPs gives rise to certain contentious concepts and themes – some extrinsic and some intrinsic - which are central to this research. These are discussed below before the researcher moves to problematise the role and liability of ISPs against these factors.

5.3.1 INTERNATIONAL OBLIGATIONS

The ISP landscape in Ireland is shaped by domestic policies and technological advancements and significantly influenced by international commitments. This section reiterates the key international treaties discussed in Chapter 2, emphasizing their implications for ISPs in Ireland.

a. Adherence to European Union Directives

As a member of the EU, Ireland must comply with various EU directives that impact the operation and regulation of ISPs. Key among these is the Digital Single Market

[409] TechArchives “How the internet came to Ireland” https://techarchives.irish/how-the-internet-came-to-ireland-1987-97/ (Date of use: 13 January 2022).

Strategy,[410] which aims to open digital opportunities for people and businesses across member states. Under this strategy, ISPs in Ireland must align with regulations that facilitate cross-border digital services, ensure consumer protection in the digital sphere, and uphold digital rights.

b. General Data Protection Regulation (GDPR)

The GDPR is a critical EU regulation with far-reaching implications for ISPs in Ireland. GDPR mandates stringent data protection and privacy standards, requiring ISPs to implement robust measures to safeguard user data. This includes obtaining explicit consent for data processing, ensuring data security, and reporting data breaches promptly. ISPs must also ensure the right to data portability and the right to be forgotten, allowing users greater control over their personal information.[411]

c. The ePrivacy Directive and Upcoming ePrivacy Regulation

The ePrivacy Directive and its forthcoming replacement, the ePrivacy Regulation, complement the GDPR by specifically addressing privacy in electronic communications. For Irish ISPs, this means adhering to rules regarding the confidentiality of communications, the handling of cookies and electronic marketing, and the security of networks and services. The upcoming ePrivacy Regulation is set to bring more clarity and modernize the rules to align with the digital age.[412]

d. Cybersecurity Directive (NIS Directive)

---

410 Enterprise.Gov "Digital Single Market" https://enterprise.gov.ie/en/what-we-do/the-business-environment/digital-single-market/ (Date of use: 13 November 2023).

411 Citizens Information "Overview of the General Data Protection Regulation" https://www.citizensinformation.ie/en/government-in-ireland/data-protection/overview-of-general-data-protection-regulation/ (Date of use: 13 December 2023).

412 Timon et al. "Data Protection Laws and Regulations Ireland 2023-2024" https://iclg.com/practice-areas/data-protection-laws-and-regulations/ireland#:~:text=The%20ePrivacy%20Regulations%20apply%20to,marketing%20from%20outside%20the%20EU. (Date of use: 12 December 2023).

The NIS Directive, or the Directive on Network and Information Systems Security, is the first piece of EU-wide legislation on cybersecurity. It requires ISPs in Ireland to take appropriate technical and organisational measures to secure their network and information systems. It also involves notifying relevant national authorities about serious cybersecurity incidents. This directive is crucial in ensuring a high common level of network and information system security across the EU.[413]

e. Telecommunications Framework Directive

The Telecommunications Framework Directive sets a regulatory framework for EU electronic communications networks and services. Irish ISPs must comply with this directive's provisions on market access, interconnection, and universal service, ensuring fair competition and consumer rights in the telecommunications sector.[414]

f. International Telecommunication Union (ITU) Regulations

Beyond EU directives, Irish ISPs also adhere to standards set by the International ITU, a UN-specialized agency for information and communication technologies. The ITU provides guidelines on a range of issues, from spectrum allocation to global telecommunications standards.[415] Compliance with ITU regulations ensures that Irish ISPs align with international best practices and contribute to the worldwide interoperability of telecommunications networks.

g. World Trade Organisation Commitments

As part of its commitments under the WTO, particularly the General Agreement on Trade in Services (GATS), Ireland must maintain specific standards in telecommunications services. This includes commitments on market access and

413 European Commission “Implementation of the NIS in Ireland” https://digital-strategy.ec.europa.eu/en/policies/nis-directive-ireland (Date of use: 12 December 2023).

414 European Commission “Implementation of the NIS in Ireland” https://digital-strategy.ec.europa.eu/en/policies/nis-directive-ireland (Date of use: 12 December 2023).

415 International Telecommunication Union (ITU), "Facts and Figures 2023 - Internet Use," https://www.itu.int (Date of use: 9 January 2024).

national treatment for foreign service providers, affecting the competitive landscape for ISPs in Ireland.

h. Budapest Convention on Cybercrime

Although not an EU directive, the Budapest Convention on Cybercrime is another significant international treaty impacting Irish ISPs. It addresses the prevention, investigation, and prosecution of cybercrime, including computer systems and data offences. ISPs in Ireland must align with these provisions, especially in assisting law enforcement agencies in investigating and preventing cybercrimes.[416]

i. Regional Agreements and Bilateral Treaties

Ireland is also a party to various regional agreements and bilateral treaties that impact ISPs. These agreements often include provisions on digital trade, cross-border data flows, and collaborative measures in technology and innovation. Compliance with these agreements ensures that Irish ISPs operate within the legal frameworks of these international partnerships.[417]

5.3.2 CONSTITUTIONAL FRAMEWORK

In Ireland, the constitutional framework significantly shapes the role and liability of ISPs, even though the Constitution does not explicitly address modern digital and internet issues. This influence is particularly evident in how ISPs balance freedom of expression and privacy rights and ensure non-discrimination in access to digital services.

The right to freedom of expression is one of the most critical constitutional principles that affect ISPs. Article 40.6.1 of the Irish Constitution outlines the liberty to express convictions and opinions, a fundamental aspect of ISP operations since they provide platforms for such expressions. However, ISPs must navigate the limitations imposed by the Constitution and other legislative measures that restrict this freedom to maintain

416 Sorbán 2019: 23.
417 Sorbán 2019: 23.

public order and morality. This responsibility includes managing and filtering online content to ensure it aligns with legal standards, making ISPs key players in the debate around online censorship and freedom of speech.[418]

The right to privacy, while not explicitly mentioned in the Irish Constitution, has been established and reinforced through judicial interpretation. This right imposes a duty on ISPs to protect users' data and maintain the confidentiality of communications. Adherence to data protection laws, particularly under the GDPR, is crucial for ISPs to respect this constitutional right. As custodians of large volumes of personal data, ISPs must ensure robust data protection measures are in place, balancing their commercial interests with the privacy rights of individuals.[419]

Equality and non-discrimination are other constitutional principles that impact ISPs. The principle of equality before the law compels ISPs to provide services without discrimination, including ensuring equitable internet access across various social and economic groups. This aspect is vital in addressing the digital divide and ensuring that internet services do not perpetuate societal inequalities.

The Irish judiciary has played a crucial role in shaping how these constitutional principles apply in the digital realm. Through various court rulings on issues like online defamation, hate speech, and illegal content, the judiciary has clarified the extent of ISPs' liabilities and responsibilities. These decisions guide ISPs in content management, outlining the conditions under which they can be held liable for the content on their platforms.[420]

Constitutional principles have also influenced several pieces of legislation that directly impact ISPs. For instance, the Defamation Act clarifies the conditions under which ISPs can be held liable for defamatory content hosted on their platforms. Similarly, data

418 Sorbán 2019: 23.
419 Sorbán 2019: 23.
420 Sorbán 2019: 23.

protection legislation influenced by the right to privacy governs how ISPs process and handle personal data.[421]

The role of ISPs in content regulation is increasingly significant in Ireland. Tasked with enforcing content standards and protecting users from online harms, ISPs find themselves in a complex regulatory environment. They must balance their responsibility to control harmful content with users' rights to freedom of expression and information. This balancing act places ISPs in a challenging position, often requiring them to make difficult decisions about content management and user rights.[422]

In the evolving digital age, ISPs face new challenges that test the application of these constitutional principles. Issues such as cyberbullying, online hate speech, and digital privacy invasions demand ISPs to continually adapt their policies and practices to keep pace with technological advancements and changing patterns of internet use.

As technology continues to evolve, so does the interpretation and application of these constitutional principles in the context of the digital environment. ISPs in Ireland must stay informed of these developments to ensure their practices comply with legal requirements and uphold the constitutional values of freedom of expression, privacy, and equality. This dynamic interplay between constitutional principles and digital technology will continue to shape the future of ISP regulation in Ireland, necessitating a continual re-evaluation and adaptation of practices and policies in this sector.

5.3.3 LEGISLATIVE FRAMEWORK

In Ireland, the legislative framework governing ISPs comprises various acts and regulations, each playing a specific role in defining the responsibilities and liabilities of

421 Sorbán 2019: 23.

422 Timon et al. “Data Protection Laws and Regulations Ireland 2023-2024” https://iclg.com/practice-areas/data-protection-laws-and-regulations/ireland#:~:text=The%20ePrivacy%20Regulations%20apply%20to,marketing%20from%20outside%20the%20EU. (Date of use: 12 December 2023).

ISPs in the digital landscape. This framework addresses direct internet governance and includes ancillary legislation that impacts the operation of ISPs.

a. **Electronic Communications Networks and Services (ECNS) Regulations**: Derived from EU Directives, these regulations provide a comprehensive framework for electronic communication services, including ISPs. They set out the licensing requirements, service provision standards, and the regulatory powers of the Commission for Communications Regulation (ComReg) in overseeing ISPs.

b. **Data Protection Acts and GDPR Implementation**: An essential piece of legislation that affects ISPs is the Data Protection Act 2018, which incorporates the EU GDPR. This act governs how ISPs process personal data and enforce data protection principles, ensuring user privacy and personal information protection.

c. **Defamation Act**: The Defamation Act 2009 is crucial for ISPs as it outlines the conditions under which they can be held liable for defamatory content hosted on their platforms. This Act balances freedom of expression with the right to protect one's reputation, imposing specific responsibilities on ISPs regarding content moderation and removal.

d. **European Union (Consumer Information, Cancellation and Other Rights) Regulations**: These regulations, derived from the EU Consumer Rights Directive, affect ISPs by setting out the information requirements and rights related to digital content. They ensure consumer protection in electronic commerce, in which ISPs are deeply involved.

e. **The Copyright and Related Rights Act**: This Act is significant for ISPs as it deals with copyright infringement issues online. ISPs must navigate these regulations to avoid liability for hosting or transmitting copyrighted material without authorization.

f. **Cybercrime Legislation**: This includes laws such as the Criminal Justice (Offences Relating to Information Systems) Act, which criminalizes unauthorized access and interference with information systems, data, and cyber fraud. ISPs must ensure their networks are secure and not used for cybercriminal activities.

g. **European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations**: This legislation governs the processing of personal data and the protection of privacy in the electronic communications sector, directly impacting ISP operations.

h. **Child Trafficking and Pornography Act**: ISPs have a duty under this Act to ensure their services are not used for the distribution or access to child pornography. This involves implementing content filters and reporting mechanisms.

i. **Criminal Justice (Money Laundering and Terrorist Financing) Acts**: These acts require ISPs, especially those involved in electronic transactions, to have measures to prevent their platforms from being used for money laundering or terrorist financing.

j. **Broadcasting Act**: Although primarily focused on broadcasting services, certain provisions of this Act impact ISPs, especially those offering streaming or on-demand services, in terms of content regulation and broadcasting standards.

k. **Ancillary Legislation**: This includes various other laws that, while not directly targeting ISPs, affect their operations. These may include business operation, taxation, consumer protection, and employment laws, which govern the broader commercial and operational environment in which ISPs function.

The legislative framework in Ireland thus presents a comprehensive and multi-faceted approach to regulating ISPs. These laws collectively address the vast issues ISPs encounter, from data protection and privacy to copyright and cybercrime, ensuring their operations align with national and EU standards. ISPs must continually monitor and

adapt to changes in this legislative environment to remain compliant and effectively serve their user base while upholding legal and ethical standards.

5.3.4 JUDICIAL INTERPRETATION

In this context, a notable aspect of the Irish judicial system is the fewer landmark decisions directly involving ISPs than in other jurisdictions. This could be attributed to several factors, including the comprehensive legislative framework that provides clear guidelines and regulations for ISP operations, reducing the frequency of contentious issues escalating to higher courts. Additionally, the complexity of digital law and the fast-paced evolution of technology might contribute to challenges in bringing cases forward, as legal frameworks are continually catching up with technological advancements.

In the cases that have been adjudicated, several themes emerge:[423]

a. **Data Protection and Privacy**: Irish courts have increasingly focused on data protection and privacy issues, especially after GDPR implementation. While not always directly involving ISPs, these cases set precedents that affect how ISPs handle personal data, emphasising user consent, data security, and the implications of data breaches.

b. **Defamation and Content Regulation**: Cases involving defamation have clarified the extent of ISP liability for user-generated content. These rulings often explore the balance between freedom of expression and protecting individual reputation, setting parameters for when ISPs must remove defamatory content upon notice.

c. **Copyright Infringement**: The judicial approach to copyright infringement cases involving ISPs has focused on the ISPs' responsibility to prevent using their networks for copyright violations. This includes assessing the adequacy of

[423] Timon et al. "Data Protection Laws and Regulations Ireland 2023-2024" https://iclg.com/practice-areas/data-protection-laws-and-regulations/ireland#:~:text=The%20ePrivacy%20Regulations%20apply%20to,marketing%20from%20outside%20the%20EU. (Date of use: 12 December 2023).

measures taken by ISPs to curb such activities and their response to copyright holders' complaints.

d. **Jurisdictional Challenges**: Some cases have highlighted jurisdictional complexities, particularly when digital content crosses national boundaries. These cases examine the applicability of Irish law to ISPs based outside Ireland but serving Irish users, reflecting the global nature of digital services and the challenges in enforcing national laws.

e. **European Union Influence**: Decisions by the Court of Justice of the European Union (CJEU) also significantly impact Irish jurisprudence in this area. While direct comparisons between the EU and SA can be complex due to different legal frameworks and market structures, CJEU rulings on digital privacy, data protection, and ISP liability influence Irish legal standards and practices.

The absence of many high-profile cases in Ireland may suggest that existing legal frameworks effectively address most issues related to ISP operations, reducing the need for judicial intervention. Alternatively, it could indicate that the complexities of digital law pose challenges in bringing matters to court or that the jurisdictional scope of Irish courts is limited in cases involving cross-border digital services.

5.4 INTERNET SERVICE PROVIDERS – PRESENT CHALLENGES

The current challenges to ISPs in Ireland include:

a. **Cybersecurity Threats**: ISPs are increasingly grappling with cybersecurity threats. These range from distributed denial-of-service (DDoS) attacks to data breaches. The escalation in cybercrimes significantly burdens ISPs to enhance security protocols and safeguard user data.[424]

[424] Timon et al. “Data Protection Laws and Regulations Ireland 2023-2024” https://iclg.com/practice-areas/data-protection-laws-and

b. **Content Regulation and Censorship**: Balancing freedom of expression with regulatory compliance presents a challenge. ISPs are often in a dilemma over decisions to block or allow content, especially content that toes the line between free speech and hate speech, misinformation, or illegal activities.[425]

c. **Data Privacy and Compliance**: ISPs must align their data processing activities with stringent privacy standards. Ensuring compliance with these regulations, particularly in evolving digital data usage, is challenging.[426]

5.5 PRELIMINARY CONCLUSION

The exploration of the role and liability of ISPs in Ireland unveils a dynamic and complex landscape. Ireland's position, deeply integrated within the EU's legal framework, particularly in digital privacy and electronic communications, significantly shapes the practices and responsibilities of its ISPs. This alignment with EU standards ensures a robust and harmonized approach to ISP regulation, especially in data protection and user privacy. Like many other jurisdictions, Ireland grapples with the delicate balance between regulating online content and preserving free speech. This balance is increasingly challenging in the digital age, where the distinction between lawful expression and harmful content is often unclear. ISPs in Ireland operate in an environment where vigilance in content management is paramount, yet they must also respect the principles of freedom of expression.

Cybersecurity and data protection are at the forefront of ISP liabilities in Ireland. The enforcement of stringent data protection laws, especially under the GDPR, places significant responsibility on ISPs to protect user data against breaches and unauthorized access. This aspect of ISP liability underscores the necessity for continuous technological adaptation and vigilance. Another key aspect of ISP operation in Ireland

regulations/ireland#:~:text=The%20ePrivacy%20Regulations%20apply%20to,marketing%20from%20outside%20the%20EU. (Date of use: 12 December 2023).

425 Sorbán 2019: 23.

426 Sorbán 2019: 23.

is the commitment to digital inclusivity and the expansion of internet accessibility. ISPs are crucial in bridging the digital divide by providing reliable and affordable internet services across diverse geographic areas, presenting operational and financial challenges.[427]

The Irish legal system has played a pivotal role in shaping ISP practices through progressive judicial interpretation and legal precedents, particularly concerning content regulation and user rights. These judicial decisions provide much-needed clarity and set precedents that guide the operations of ISPs. Looking forward, the role and liability of ISPs in Ireland are expected to continue evolving, influenced by technological advancements, changing user expectations, and legal developments. The comparative analysis brings similarities and differences in ISP regulation across jurisdictions. This comparison is invaluable for identifying best practices and potential areas for global legal and policy reforms in ISP governance.

In the next chapter, the researcher examines and compares the role and liability of ISPs in Nigeria.

[427] Lembani et al. 2020: 74.

CHAPTER SIX

THE ROLE AND LIABILITY OF INTERNET SERVICE PROVIDERS IN NIGERIA

6.1 INTRODUCTION

This chapter embarks on a comprehensive exploration of the role and liability of ISPs in Nigeria. The examination is anchored in a comparative context, seeking to juxtapose Nigeria's regulatory and operational dynamics of ISPs with those of South Africa. This comparative approach aims to delineate the distinct characteristics of Nigeria's ISP landscape and potentially unearth valuable insights, lessons, and good practices that might enhance the South African context.

Nigeria, Africa's most populous nation and one of its largest economies presents a unique case study in digital communication and internet services. The country's approach to managing and regulating ISPs is deeply influenced by its socio-economic, political, and cultural nuances. Understanding these influences is key to comprehending the liabilities and responsibilities imposed upon ISPs within the Nigerian digital ecosystem.

The researcher aims to delve into the intricacies of Nigeria's legal and regulatory frameworks governing ISPs, examining how these frameworks shape the services provided to end-users and the content they access. This exploration includes an analysis of the Nigerian legal system's stance on digital rights, data protection, and content regulation, as well as the operational challenges faced by ISPs in this dynamic environment.

Furthermore, this chapter explores the interplay between Nigerian ISPs and international standards and obligations, particularly focusing on how global internet governance trends impact local practices. Examining Nigeria's compliance with international

cybersecurity norms, data protection standards, and content regulation policies is crucial for understanding the broader context in which Nigerian ISPs operate.

Another critical aspect of this chapter is the exploration of the practical implications of the legal and regulatory environment for ISPs in Nigeria. This includes scrutinizing the balance between fostering digital innovation and entrepreneurship and ensuring user safety and data privacy. The role of ISPs in bridging the digital divide, a significant challenge in the Nigerian context, is also a key focus area.

This chapter aims to contribute to the body of knowledge on Internet governance and ISP liability. By drawing comparisons with South Africa and highlighting the unique aspects of the Nigerian scenario, this research aims to inform policy action, enhance academic understanding, and potentially guide future legal reforms in the rapidly evolving digital landscape.

6.2 INTERNET SERVICE PROVIDERS – HISTORICAL DEVELOPMENT

The historical development of ISPs in Nigeria, a former British colony, reflects a unique interplay of colonial legacy, post-independence policies, and the rapid global technological evolution. This section traces the trajectory of ISP development in Nigeria, contextualizing it within the broader legal and socio-political evolution framework.

During colonial times and the early years following independence in 1960, Nigeria's telecommunications infrastructure was rudimentary, primarily serving the administrative needs of the colonial and early post-colonial governments.[428] The focus was more on essential telecommunication than Internet services, as the Internet was not yet a global phenomenon. The Nigerian Telecommunications Limited (NITEL), a state-owned monopoly, dominated this era, providing limited telecommunication services.

[428] Jemilohun 2019: 353.

The significant shift in Nigeria's ISP landscape began in the late 20th century, coinciding with global digital advancements. The 1990s marked the beginning of Nigeria's telecommunications revolution, characterized by the liberalization and privatization of the telecom sector. This period saw the Nigerian government, under the Structural Adjustment Program encouraged by the World Bank and IMF, enacting policies to end the monopoly of NITEL and open the market to private players.[429]

The Telecommunications Sector Reform Act of 1992 was a landmark, paving the way for private participation and the introduction of mobile telephony. However, the internet component of telecommunications was still in its infancy.[430]

The internet boom hit Nigeria in the late 1990s and early 2000s by establishing the first ISPs. These early ISPs were primarily focused on urban areas, offering dial-up services. The government, recognizing the potential of the Internet for national development, embarked on policy reforms to foster a conducive environment for ISP growth.[431]

The Nigerian Communications Commission (NCC), established in 1992, played a pivotal role in regulating and promoting the ISP industry. The Nigerian Communications Act in 2003 further liberalized the sector, leading to an influx of private ISPs and a competitive market.[432]

The last decade has seen a significant shift towards broadband internet, driven by the global shift to high-speed internet services. Nigeria's National Broadband Plan launched in 2013 and revised recently, aims to increase broadband penetration nationwide, emphasizing the need for affordable and accessible internet services.[433]

This era has seen the rise of major ISPs like MTN, Glo, Airtel, and 9mobile, which have expanded their services beyond mobile telephony to broadband internet. The

429 Ifonlaja 2023: 11.
430 Jemilohun 2019: 353.
431 Jemilohun 2019: 353.
432 Jemilohun 2019: 353.
433 Ifonlaja 2023: 11.

government's focus has also shifted to issues like cyber security, online content regulation, and digital rights, reflecting global concerns in internet governance.[434]

Nigeria's legal framework for ISPs has evolved to address the challenges of the digital age. Laws like the Cybercrimes Act of 2015 and the Nigeria Data Protection Regulation of 2019 have been enacted to address cyber security, data protection, and privacy issues in the digital space. These laws also delineate the responsibilities and liabilities of ISPs in protecting user data and curbing cybercrimes.[435]

It is trite that despite significant growth, the Nigerian ISP sector faces challenges such as infrastructural deficits, especially in rural areas, and regulatory hurdles. Moreover, issues like internet censorship, digital rights, and affordability remain areas of concern. Nigeria's ISP industry appears poised for further growth, driven by ongoing policy reforms, technological advancements, and increasing digital literacy. The government's commitment to improving broadband access and fostering a digitally inclusive society will shape the future trajectory of ISPs in Nigeria.

6.3 CONTEMPORARY THEMES

The contemporary structure for regulating ISPs gives rise to certain contentious concepts and themes – some extrinsic and some intrinsic - which are central to this research. These are discussed below before the researcher moves to problematise the role and liability of ISPs against these factors.

6.3.1 INTERNATIONAL OBLIGATIONS

As a global participant, Nigeria is subject to various international treaties and agreements that directly or indirectly influence ISP operations and liabilities within its jurisdiction. These international obligations, initially detailed in Chapter 2,[436] are crucial

[434] Ifonlaja 2023: 11.
[435] Jemilohun 2019: 353.
[436] The references and citations applied in chapter 2 on this aspect are considered to apply here without change.

in shaping the regulatory landscape for ISPs in Nigeria. This section reiterates these treaties and their impact on Nigerian ISPs.

Nigeria is a member of the ITU, which sets global standards for telecommunications, including internet services. Nigeria's ITU commitments align its ISP regulations with international standards covering various aspects, from spectrum allocation to cybersecurity measures. Participation in the WSIS further commits Nigeria to global discussions and policies regarding the internet, impacting its domestic ISP regulatory framework.

Nigeria has obligations concerning telecommunications services under the WTO and various bilateral and multilateral trade agreements. These agreements impact how Nigeria regulates its telecommunications market, including ISPs, especially regarding market access for foreign service providers and investment. The GATS under the WTO framework, for example, influences the competitive landscape for Nigerian ISPs by dictating how the country opens its telecommunications sector to international players.

Nigeria's approach to ISP regulation is shaped by its stance on cybercrime and data protection. While not a signatory to the Budapest Convention on Cybercrime,[437] the principles and guidelines of this convention influence global norms and practices, including those in Nigeria. The adoption of the Nigeria Data Protection Regulation (NDPR) in 2019, which mirrors aspects of the EU’s GDPR, reflects Nigeria's alignment with international data protection standards. ISPs operating in Nigeria must comply with these data protection standards, particularly concerning the handling of user data.

Nigeria is influenced by the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) as part of the African Union. This convention aims to harmonize cybersecurity and data protection laws across Africa, impacting Nigerian ISPs' regulatory environment. Compliance with the Malabo Convention means that

[437] Ifonlaja 2023: 14.

Nigerian ISPs must align with regional commitments, ensuring consistency in digital policies across the continent.

Nigeria’s obligations under international human rights treaties, such as the ICCPR, have implications for ISP operations, particularly regarding freedom of expression and privacy. While Nigeria balances these rights with national security and public order considerations, ISPs are often at the intersection of facilitating free expression and adhering to state-imposed limitations.

Nigeria's commitment to the UN’s SDGs, particularly Goal 9, which emphasizes the role of infrastructure and innovation, including ICT, also guides its ISP policies. This commitment is reflected in efforts to enhance ISP services for broader and more equitable internet access.

Nigeria's international obligations significantly shape its ISP regulatory framework. These obligations ensure Nigerian ISPs comply with global standards and contribute to broader economic growth, technological advancement, and societal development goals. As Nigeria continues to navigate its place in the global digital ecosystem, the role of ISPs in upholding these international commitments remains pivotal. Balancing these international obligations with domestic priorities will continue to be a dynamic and evolving process for Nigerian policymakers and ISPs.

6.3.2 CONSTITUTIONAL FRAMEWORK

Nigeria's constitutional framework provides the legal foundation for regulating and operating ISPs. This framework includes various constitutional provisions significantly impacting ISPs' roles, responsibilities, and liabilities regarding content producers and end-users. This section delves into analyzing and discussing these pertinent constitutional provisions.

The Constitution of the Federal Republic of Nigeria guarantees fundamental human rights, which are crucial for ISPs. The right to freedom of expression is particularly relevant, enshrined in section 39. This section provides for the freedom to hold opinions,

receive ideas and information without interference, and impart ideas and information through any media. ISPs, as facilitators of digital communication, play a critical role in upholding this freedom. However, they must also navigate the complexities of content regulation, ensuring they do not become tools for unlawful censorship or infringement of users' rights.

Section 37 of the Nigerian Constitution guarantees the right to privacy, including communication privacy. This provision directly impacts ISP handling and protecting of user data and communications. ISPs ensure that users' personal and communication data are not arbitrarily accessed or used without consent, aligning their operations with constitutional privacy protections.

The constitutional framework provides the basis for legislative and regulatory measures governing ISPs. Laws such as the Nigerian Cybercrimes Act of 2015, established within the constitutional boundaries, impose specific obligations on ISPs concerning cybercrime prevention and reporting.[438] These include mandates on data retention and disclosure of user information to lawful authorities under certain conditions, balancing these requirements with constitutional rights.

While the Constitution guarantees freedoms and rights, it also allows for lawful restrictions in the interest of national security, public order, morality, and others' rights. ISPs in Nigeria operate within this constitutional context, often required to comply with government directives that may involve surveillance or blocking access to certain digital content. They must strike a balance between adhering to these legal requirements and protecting users' constitutional rights.

The constitutional principle of equality and non-discrimination under section 42 has implications for ISPs. They are expected to contribute to bridging the digital divide by providing equitable access to internet services. This principle aligns with Nigeria's policy

[438] Sorbán 2019: 19-20.

objectives to enhance digital inclusion and ensure internet services are accessible to all population segments.

The Nigerian judiciary's interpretation of the Constitution further shapes the regulatory environment for ISPs. Courts can interpret constitutional provisions and adjudicate cases involving ISPs, particularly in freedom of expression, privacy, and regulatory compliance disputes. These judicial interpretations help clarify the extent of ISPs' responsibilities and liabilities under the Constitution.

The constitutional framework in Nigeria sets the legal boundaries within which ISPs must operate. It establishes the rights and freedoms that ISPs must respect and uphold and delineates their responsibilities and the scope of permissible regulation. As the digital landscape evolves, interpreting and applying these constitutional provisions in the context of ISP operations will continue to be a critical area of legal and regulatory development in Nigeria. Balancing constitutional rights with regulatory obligations remains a dynamic challenge for ISPs in Nigeria, requiring continual adaptation and compliance with the Constitution's letter and spirit.

6.3.3 LEGISLATIVE FRAMEWORK

Nigeria's legislative landscape comprises several statutes that directly or indirectly regulate the operations and responsibilities of ISPs. This legislative framework shapes how ISPs conduct their business, interact with users, and comply with national regulations. The following is an overview of the primary pieces of legislation relevant to ISPs in Nigeria, encompassing direct regulations and ancillary laws that influence their operation.

a. Nigerian Cybercrimes Act of 2015

This is a key piece of legislation that directly impacts ISPs. It addresses cybercrimes and outlines measures for cybersecurity. The Act imposes specific obligations on ISPs to prevent cybercrimes, mandates reporting of cyber incidents, and sets guidelines for cooperation with law enforcement agencies.

b. Nigerian Communications Act of 2003

As Nigeria's fundamental law governing telecommunications, this Act provides the regulatory framework for ISPs. It establishes the roles and responsibilities of the Nigerian Communications Commission (NCC) in licensing and regulating ISPs. The Act also sets standards for service provision and consumer protection.

c. The Nigerian Data Protection Regulation (NDPR) of 2019

Enacted by the National Information Technology Development Agency (NITDA), this regulation governs data privacy and protection. ISPS must manage user data, ensure data privacy, and outline data breach notification requirements.

d. Freedom of Information Act 2011

This Act promotes transparency and the right to information. It is relevant to ISPs in the context of content management and the balancing of users' rights to access information with privacy and security considerations.

e. The Child Rights Act of 2003

This Act provides for the rights and welfare of children, including in digital spaces. ISPs must ensure that their services do not facilitate the violation of children's rights and are compliant with provisions regarding child protection online.

f. Consumer Protection Framework

This includes various consumer protection laws and regulations that apply to ISPs, ensuring they provide services in a manner that protects consumers' interests. This encompasses fair billing practices, quality of service standards, and redress mechanisms for consumer grievances.

g. Anti-Terrorism Act of 2011

Under this Act, ISPs may be required to assist in combating terrorism, including surveillance and data provision measures as per lawful requests. This Act obligates ISPs to ensure their platforms are not used for terrorist activities.

h. Economic and Financial Crimes Commission (Establishment) Act, 2004

This Act, which established the EFCC, has implications for ISPs, especially in addressing internet fraud and financial crimes conducted via online platforms.

i. National Information Technology Development Agency Act 2007

This Act established NITDA, which plays a pivotal role in formulating policies and regulations for information technology, including guidelines that affect ISP operations.

j. Copyright Act of 1988

Relevant for ISPs, this Act governs intellectual property rights online, including content hosted or transmitted by ISPs. It places an onus on ISPs to respect copyright laws and prevent the dissemination of pirated materials.

k. Ancillary Legislation and Regulations

This includes other laws and regulations indirectly impacting ISPs, such as business operations, taxation, online commerce, and labour laws.

The legislative framework in Nigeria presents a comprehensive structure governing the operation of ISPs. These laws collectively address various aspects of ISP operation, from cybersecurity, data protection, and consumer rights to compliance with national security and child protection standards. ISPs in Nigeria must navigate this complex legal landscape, ensuring compliance with specific laws targeting digital communication and broader statutes that indirectly influence their operations. As the digital sector continues to evolve, these laws are subject to amendments and reinterpretation, necessitating that ISPs remain vigilant and adaptable to the changing legal environment.

6.3.4 JUDICIAL INTERPRETATION

Between 2018 and 2023, Nigerian High Courts dealt with a limited number of cases directly implicating ISPs. This scarcity could be attributed to several factors, including the relative novelty of comprehensive cyber legislation in Nigeria and the complex nature of cyber law, which might deter litigants from pursuing complex and uncharted legal battles. Additionally, the jurisdictional challenges and the rapidly evolving technology landscape could contribute to the dearth of cases at the higher judiciary levels.

In the few cases that have reached the Nigerian High Courts, the focus has been primarily on issues like defamation, data privacy breaches, and unauthorized content distribution. In these cases, ISPs have been scrutinized for their role in facilitating or failing to prevent the dissemination of harmful or illegal content. The courts have upheld the principles in the Cybercrimes Act of 2015 and the NDPR of 2019, emphasizing ISPs' responsibilities in maintaining a safe digital environment.

One notable aspect of these rulings is the emphasis on ISPs' duty to exercise reasonable care in monitoring and controlling the content transmitted through their networks. In certain instances, the courts have held ISPs accountable for lapses that led to breaches of user privacy or the spread of defamatory content. However, applying these principles has not been consistent, reflecting the evolving understanding of ISPs' roles and liabilities.[439]

One of the significant challenges in judicial interpretation in Nigeria is balancing freedom of expression with regulatory compliance. The courts have grappled with delineating ISPs' responsibilities in censoring content without overstepping into the domain of unlawful censorship or violation of free speech. This dilemma is particularly pronounced in cases involving political content or speech that borders on national security concerns.[440]

---

439 Ifonlaja 2023: 17.
440 Ifonlaja 2023: 17.

Another challenge lies in applying international legal standards and treaties, to which Nigeria is a party, in the context of domestic ISP regulations. The courts have occasionally referenced international norms in their judgments, but a need for more explicit integration of these standards into Nigerian cyber law jurisprudence remains.[441]

The absence of Supreme Court or Court of Appeal precedents on ISP-related issues indicates either a lack of appeal in such cases or a cautious approach by the higher judiciary in dealing with complex cyber law issues. This gap in jurisprudence leaves several legal questions unanswered, particularly regarding the extent of ISPs' liability in cybercrime cases and the limits of their obligations under data protection laws.

6.4 INTERNET SERVICE PROVIDERS – PRESENT CHALLENGES AND LEGISLATIVE RESPONSE

The landscape for ISPs in Nigeria is continually evolving, marked by unique challenges that arise from the country's socio-economic, technological, and legal frameworks. The rate of incidences involving cybercrimes, data breaches, and content regulation violations has prompted both legislative and practical responses aimed at shaping the role and liabilities of ISPs.

One of the most pressing challenges for Nigerian ISPs is the rising incidence of cybercrimes. As digital connectivity expands, ISPs become increasingly targeted by cybercriminals and inadvertently facilitate cybercrimes, ranging from financial fraud to data theft.[442] The Cybercrimes Act of 2015, which addresses various cyber offences and prescribes penalties, places a significant responsibility on ISPs to secure their networks and report cybercrimes. However, implementing this act remains challenging due to technological limitations, lack of awareness, and insufficient cybersecurity infrastructure among some ISPs.

441 Ifonlaja 2023: 17.
442 Ifonlaja 2023: 20.

With the enactment of the NDPR in 2019, ISPs are under a legal obligation to protect user data. The increasing data breaches and privacy concerns have put ISPs under scrutiny. Compliance with NDPR mandates ISPs to adopt data protection and privacy measures, conduct data protection impact assessments, and report data breaches. However, compliance is uneven across providers, and the capacity to enforce these regulations effectively is still developing.[443]

Another challenge is balancing content regulation with freedom of expression. ISPs are sometimes caught in the crossfire between government directives to block or filter certain online content and the public's right to information and free expression. The lack of clear guidelines and the risk of over-censorship or under-regulation make this a complex area for ISPs.

Despite significant improvements, Nigeria still faces challenges related to internet infrastructure, especially in rural and underserved areas.[444] The uneven distribution of connectivity affects the ISPs' ability to provide stable and uniform services across the country. Legislative responses, including policies to boost infrastructure development and reduce the digital divide, have been initiated but require more consistent implementation and investment.

Nigeria's commitment to international treaties and standards in cyber law and data protection also presents challenges for ISPs. Aligning domestic operations with international standards while catering to local legal and socio-economic conditions is a delicate balance that ISPs must maintain.

The rapid emergence of new technologies like 5G, IoT, and cloud computing presents opportunities and challenges for ISPs. Adapting to these technologies requires significant investment and regulatory adjustments. The legislative response has been

443 Ifonlaja 2023: 14.
444 Ifonlaja 2023: 14.

reactive, and there is a need for more proactive policies that anticipate future technological trends and their implications for ISPs.

ISPs in Nigeria also face challenges related to consumer protection and quality of service. Issues like service outages, unfair billing practices, and consumer complaints are prevalent. The NCC has been actively involved in regulating these aspects, but there remains a need for more vigorous enforcement and consumer awareness initiatives.

In conclusion, Nigerian ISPs are navigating a complex environment marked by cybersecurity risks, data protection obligations, content regulation dilemmas, infrastructural gaps, and the need to align with international standards. The legislative response has been evolving to address these challenges, but gaps in enforcement, technological capabilities, and consumer protection remain. The future landscape for ISPs in Nigeria will be shaped by how effectively these challenges are addressed through collaborative efforts between the government, ISPs, and other stakeholders in the digital ecosystem.

6.5 PRELIMINARY CONCLUSION

As the research in this chapter draws to a close, it becomes evident that the role and liability of ISPs in Nigeria are influenced by myriad factors stemming from legal, socio-economic, and technological realms. The study has navigated the historical development of ISPs in Nigeria, scrutinizing their evolution and emerging challenges. This examination has laid the groundwork for a comprehensive understanding, which will be instrumental in formulating the conclusive research results and recommendations in the forthcoming chapter.

The exploration of Nigeria's legislative framework, international obligations, and constitutional provisions related to ISPs highlights a regulatory landscape striving for balance between advancing technological innovation, protecting user rights, and ensuring national security and social order. The legislative efforts, though commendable,

reveal gaps in implementation and enforcement, especially concerning cybersecurity, data privacy, and content regulation.

In cybersecurity, the increasing incidence of cybercrimes poses a significant challenge.[445] The Cybercrimes Act of 2015, while a pivotal step towards addressing these issues, requires more robust implementation and ISP compliance. Data protection, propelled by the NDPR, underscores the ISPs' critical role in safeguarding user data. However, uniformity in adherence to these regulations across all ISPs remains challenging.

Content regulation presents a delicate balancing act for ISPs, where they must navigate between adhering to government directives and upholding the users' rights to information and free expression. This area, particularly, calls for clearer guidelines and a judicious approach to avoid over-censorship.

The infrastructural challenges, particularly in rural and underserved areas, impact the ISPs' ability to deliver consistent and reliable services, highlighting the need for more focused investment and policy implementation in this sector.[446] Moreover, aligning Nigeria's ISP operations with international standards is a continuous process that requires dynamic policy-making and technological adaptation.

As the research proceeds to the final chapter, these findings lay a solid foundation for drawing comprehensive conclusions and formulating recommendations. The subsequent chapter will synthesize these insights, addressing the primary research questions and objectives. It will delve into providing actionable recommendations that could aid in refining the regulatory and operational landscape for ISPs in Nigeria.

These recommendations will address the identified challenges, enhancing cybersecurity measures, ensuring robust data protection, promoting fair content regulation, closing infrastructural gaps, and aligning with international standards. Additionally, the

445 Sorbán 2019: 25.
446 Major 2021: 19.

recommendations will consider consumer protection and service quality as crucial aspects of ISP operations.

The final chapter promises to encapsulate the essence of this research, offering a roadmap for policymakers, ISPs, and other stakeholders. The goal is to contribute to a more secure, equitable, and progressive digital landscape for South Africa. ISPs are pivotal in driving innovation while safeguarding user rights and adhering to national and international legal standards.

CHAPTER SEVEN

CONCLUSION(S) AND RECOMMENDATIONS

7.1 INTRODUCTION

In this concluding chapter, the researcher returns to the research questions posed in chapter one and answers them based on the comparative research in the preceding six chapters. The researcher also makes certain recommendations for the consideration of the South African legislature regarding the role and liability of ISPs in South Africa.

7.2 CHAPTER SUMMARY

Chapter One: Conceptualisation and Methodology

In the first chapter, the researcher established the foundation of the study by presenting the research topic and framing the approach, research questions, and methodology. This chapter served as a roadmap, outlining the primary objectives and the scope of the research. Central research questions were introduced, providing clarity and focus for the investigation. The researcher also offered detailed definitions for key terms, drawing from South African internet jurisprudence, relevant legislation, and comparative international contexts. This groundwork was essential for setting the stage for an in-depth comparative study of the role and liability of ISPs across different jurisdictions.

Chapter Two: Internet Service Providers – Historical & Contextual Perspectives

Chapter Two delved into the global landscape of ISPs, examining their evolution and regulatory challenges within the international legal framework. The researcher explored the development of ISPs from a non-jurisdictional perspective, providing a historical overview and contextualizing their role in the international legal sphere. This chapter also addressed the global challenges ISPs face, setting the stage for a comparative analysis with specific jurisdictions.

Chapter Three: The Role and Liability of Internet Service Providers in South Africa

In the third chapter, the focus shifted to the South African context. The researcher analyzed the role and liability of ISPs in South Africa, examining constitutional provisions, relevant legislation, case law, and statutory interpretation. This chapter offered an overview of South Africa's approach to internet governance, highlighting the intricate balance between regulation, digital rights, and the country's commitment to global internet standards.

Chapter Four: The Role and Liability of Internet Service Providers in China

Chapter four presented a comparative study of ISPs in China. The researcher explored China’s unique approach to internet regulation, highlighting the interplay between state control and the growing ISP market. This chapter analyzed China's constitutional framework, legislative measures, and judicial interpretations, offering insights into how China navigates its digital landscape amidst global connectivity and national control dynamics.

Chapter Five: The Role and Liability of Internet Service Providers in Ireland

In the fifth chapter, the researcher examined the role and liability of ISPs in Ireland. This chapter critically analyzed Ireland's legislative and constitutional framework concerning ISPs. The discussion included recent developments, challenges, and judicial interpretations, offering a nuanced understanding of how Ireland regulates its digital space and protects digital rights.

Chapter Six: The Role and Liability of Internet Service Providers in Nigeria

The sixth chapter focused on Nigeria, offering an overview of the country's approach to ISP regulation. The researcher explored the historical development of ISPs, international obligations, constitutional and legislative frameworks, and judicial interpretations. This

chapter underscored the challenges and advancements in Nigeria's digital governance, providing a valuable African perspective in the comparative study.

7.3 ANSWERING THE RESEARCH QUESTIONS

Drawing from the comprehensive analysis in the preceding chapters, the researcher now addresses the original research questions. These questions are answered based on the comparative research across the different jurisdictions explored:

1. **How do different jurisdictions approach the regulation of ISPs?**

The study revealed diverse approaches to ISP regulation. South Africa and Ireland, for instance, demonstrate a balance between regulation and digital rights, while China shows a model of stringent state control. Nigeria's approach reflects a growing digital landscape with unique challenges and regulatory efforts.

2. **What are the common challenges faced by ISPs in these jurisdictions?**

Common challenges include cybersecurity threats, data privacy concerns, content regulation, and balancing user rights with national security. Each jurisdiction addresses these challenges within its unique legal and socio-political context.

3. **How do legislative and judicial frameworks impact ISPs' operations?**

Legislative and judicial frameworks significantly influence ISP operations. Laws and court rulings define ISP responsibilities in all studied jurisdictions, from content monitoring to user data protection. Judicial interpretations play a critical role in clarifying ISP legal obligations.

4. **What lessons can be learned from these jurisdictions to improve ISP regulation in South Africa?**

Lessons for South Africa include clear and enforceable regulations, robust data protection laws, and balancing state control with digital freedoms. The comparative

study highlights the benefits of learning from diverse models to refine South Africa's approach to ISP regulation.

5. **How do the current legal and regulatory frameworks in South Africa govern the operations and liabilities of ISPs, especially concerning cybercrime and online content?**

This study examined how the current legal and regulatory frameworks in South Africa govern the operations and liabilities of ISPs, especially concerning cybercrime and online content. It provided a thorough analysis rooted in a comparative perspective with China, Ireland, and Nigeria.

A blend of statutory and common law principles underpins South Africa's approach to ISP regulation. Central to this framework is the ECTA, which explicitly addresses cybercrime and outlines the responsibilities of ISPs in preventing and reporting cybercrimes. This Act and the POPIA establish a legal obligation for ISPs to safeguard user data and maintain robust cybersecurity measures. Moreover, these laws delineate the extent of ISP liability in data breaches and illegal online activities, positioning ISPs as service providers and as crucial gatekeepers in the digital security landscape.

While comprehensive in terms of legislative scope, South Africa's approach faces challenges in practical implementation. The rapid evolution of technology often outpaces the legislative process, creating gaps in the legal framework that can be exploited. Furthermore, the balance between protecting user rights, such as privacy and freedom of expression, and enforcing laws against cybercrime and harmful content is delicate. The legal system sometimes struggles to keep up with the dynamic and borderless nature of the internet, leading to difficulties in enforcing regulations effectively.

The judicial interpretation of these laws has been pivotal in defining the scope of ISP liability. Landmark cases have shaped the understanding of reasonable measures for

ISPs to prevent and report cybercrime. However, the courts have also recognized the limitations of ISPs in monitoring and controlling all content on their platforms. This judicial perspective underscores the necessity of ISPs to operate within a defined legal framework while acknowledging the practical limitations of their role.

Comparatively, South Africa's framework shares similarities with the approaches in Ireland and Nigeria, particularly in the emphasis on data protection and the fight against cybercrime. However, unlike China's more centralized and stringent control over ISPs, South Africa's model aligns more with global internet governance standards, balancing state interests with individual rights.

6. **How do the legal systems and internet governance models in China, Ireland, and Nigeria differ from South Africa regarding ISP regulation, and what lessons can be learned from these jurisdictions?**

China’s model is characterized by stringent state control and extensive regulation of ISPs. The Chinese government employs a comprehensive legal framework that mandates ISPs to adhere to strict content filtering and surveillance guidelines. This approach is primarily influenced by the government's priority on national security and social stability. Unlike South Africa's liberal approach, China's model is more restrictive, with significant implications for freedom of expression and privacy. The lesson from China’s model is the effectiveness of a centralized regulatory system in controlling online content, but at the cost of individual freedoms, which may not align with the democratic values upheld in South Africa.

EU directives guide Ireland's ISP regulation approach and emphasise data protection, privacy, and freedom of expression. Irish ISPs operate under a legal framework that balances user rights with the responsibility to manage harmful online content. Compared to South Africa, Ireland’s model benefits from being part of the EU, which provides a cohesive regulatory environment and access to a broader set of resources and expertise. The critical lesson for South Africa could be the advantage of aligning

with larger international regulatory frameworks to enhance the effectiveness of ISP regulation.

Sharing similarities with South Africa as a developing country, Nigeria focuses on developing its digital infrastructure while tackling cybercrime. The Nigerian model is evolving, with laws and regulations to protect users and ensure responsible internet use. The country faces challenges like South Africa, such as balancing regulation with promoting digital freedoms. Nigeria's ongoing efforts to update its legal framework in response to technological changes can be a valuable lesson for South Africa in adapting and evolving its regulatory approach. The study highlights significant differences in how these countries regulate ISPs. China's model is heavily centralized and controlled, Ireland benefits from its EU membership, and Nigeria, like South Africa, is navigating the complexities of evolving digital landscapes in a developing country context.

From these jurisdictions, South Africa can learn the importance of striking a balance between effective regulation and the preservation of digital freedoms. While effective in control, the Chinese model may be too restrictive for South Africa's democratic context. Ireland's approach, rooted in EU frameworks, offers insights into harmonizing regulations with broader international standards, which South Africa could consider for regional collaborations in Africa. Nigeria's evolving framework reflects a context like South Africa's, highlighting the importance of continuous legal adaptation and capacity building in ISP regulation. Examining these diverse models provides South Africa with a spectrum of regulatory approaches to ISP governance. The lessons learned can guide South Africa in refining its regulatory framework to ensure it remains effective, adaptable, and aligned with national objectives and international best practices.

7. **How effective are the existing laws in South Africa in achieving their intended objectives of deterring cybercrime, protecting user privacy, and upholding freedom of expression?**

The effectiveness of existing laws in South Africa in deterring cybercrime, protecting user privacy, and upholding freedom of expression presents a multifaceted picture. Each of these objectives, while interrelated, demands a unique approach within the legal framework, leading to varied levels of success. South African laws have made significant strides in addressing cybercrime. The enactment of the Cybercrimes Act, for instance, has been a crucial step in defining and criminalizing various online offences. This Act provides clear legal recourse for cybercrimes, ranging from data breaches to cyber fraud. However, the challenge remains in enforcement. The rapid evolution of technology and the sophistication of cybercriminals often outpace legal and law enforcement capabilities. While the statutes set a solid foundation, their effectiveness is hampered by the need for continuous updates and the development of specialized enforcement units.

The POPIA has been a landmark regarding privacy laws in South Africa. It aligns with international standards, particularly the GDPR, in safeguarding personal data. POPIA imposes strict obligations on ISPs and other entities handling personal data, ensuring user privacy is respected and protected. However, the real test of effectiveness lies in the implementation and compliance. The Act requires ongoing awareness and capacity building among stakeholders, and while it's a robust framework on paper, its practical impact is still consolidating.

With its strong constitutional commitment to freedom of expression, South Africa has laws supporting this right in the digital realm. However, balancing this freedom with other objectives, such as preventing hate speech and disinformation, presents ongoing challenges. Laws regulating online content must tread carefully to avoid overreach that could stifle free speech. The challenge lies in crafting regulations that adequately address harmful online behaviour without intruding on the fundamental right to freedom of expression. The overarching challenge in South Africa's legal framework for ISPs is finding a harmonious balance between these objectives. Effective cybersecurity measures sometimes conflict with privacy concerns, and both can intersect with the boundaries of free expression. Additionally, the global nature of

the internet means that South Africa's laws must be adaptable and responsive to international trends and threats.

While South Africa’s existing laws demonstrate a commendable effort in addressing the complex issues of cybercrime, privacy, and freedom of expression, their effectiveness is evolving. Continuous assessment, amendment, and education ensure these laws reflect the current digital landscape and are practical and enforceable. Collaborative efforts between the government, ISPs, legal experts, and the community are essential in adapting to the dynamic nature of the Internet and ensuring that the legal framework achieves its intended objectives.

8. **What are the implications of ISP regulation for consumers, the government, and ISPs regarding rights, responsibilities, and business operations?**

The regulation of ISPs in South Africa has a multifaceted impact on various stakeholders, including consumers, the government, and the ISPs themselves. These impacts are interconnected and influence the country's overall digital landscape.

For consumers, the primary impact is on their data protection and online safety. Regulations like POPIA enhance consumer protection by giving users more control over how their information is collected, processed, and stored. This shift towards greater data privacy is crucial in building trust in the digital economy. However, stringent content regulation might also limit access to certain types of information, affecting consumers' right to information and freedom of expression. Furthermore, the cost of compliance with these regulations by ISPs might lead to increased service charges, impacting consumer affordability.

From the government's perspective, regulating ISPs presents challenges and opportunities. The government is tasked with updating and enforcing regulations in a rapidly evolving technological environment, requiring constant vigilance, adaptability, and investment in expertise. One of the biggest challenges is balancing protecting consumers and maintaining national security without stifling innovation and infringing

on digital freedoms. The enforcement of these regulations, particularly in combating cybercrimes and data breaches, demands substantial resources and specialized knowledge.[447]

ISPs, on the other hand, face a complex set of responsibilities and challenges under the regulatory framework. Adherence to regulations often entails high costs, including investments in secure infrastructure and compliance programs. This can be burdensome for smaller ISPs, affecting the competitive dynamics in the sector. ISPs must adjust their operations to comply with regulations, which might involve changing how they handle user data, respond to government requests, and manage content on their platforms. Additionally, the increased responsibility and liability, especially concerning user data protection and content management, pose legal and operational risks that require robust management strategies.

Therefore, the implications of ISP regulation in South Africa are extensive and multifaceted. It translates into better protection for consumers but potentially at a higher cost. For the government, it involves a continuous balancing act of regulating while fostering a conducive environment for digital innovation. For ISPs, it demands navigating a landscape of compliance, operational adjustments, and increased responsibilities. The effectiveness of these regulations in achieving their intended objectives and their impact on technological innovation and freedom of expression is a delicate balance that needs ongoing assessment and collaboration among all stakeholders.

9. How do technological advancements and ethical concerns influence the regulation of ISPs, and what challenges do these factors pose for effective governance?

Technological advancements and ethical concerns significantly influence the regulation of ISPs and pose unique challenges to effective governance. The rapid

447 Zingales 2019: 14.

pace of technological innovation often outstrips existing regulatory frameworks, creating a dynamic where regulations are perpetually trying to catch up with new realities. This scenario is evident in data protection, content regulation, and cybersecurity.

Firstly, technological advancements have led to an exponential increase in the volume and variety of data generated and collected by ISPs. This data proliferation raises significant privacy concerns, necessitating robust data protection regulations. Regulators must devise flexible laws to adapt to evolving technologies while providing sufficient user data protection. For instance, the rise of cloud computing and the Internet of Things (IoT) has complicated data sovereignty and security issues. Ensuring ISPs comply with data protection regulations while leveraging these technologies for improved services is a delicate balance.

Moreover, the ethical implications of content moderation and censorship by ISPs have become increasingly complex. With the advent of artificial intelligence and machine learning, ISPs have more tools for content filtering. However, this raises ethical concerns regarding censorship, freedom of expression, and the potential for algorithmic bias. Regulators face the challenge of establishing guidelines that protect against harmful content while respecting free speech and preventing the overreach of automated content moderation systems. Cybersecurity is another area where technological advancements significantly impact ISP regulation. The increasing sophistication of cyber threats requires ISPs to adopt advanced security measures to protect their networks and users. However, this also means that ISPs must continually invest in new technologies and expertise to stay ahead of cybercriminals. Regulators must ensure that ISPs implement robust cybersecurity measures and actively update them in response to new threats.

Another challenge is the global nature of the Internet, which means that ISPs often operate across multiple jurisdictions with varying regulatory requirements. This situation creates a complex legal landscape where ISPs must navigate different laws

and standards, particularly concerning data protection and user privacy. Finally, ethical concerns related to user rights, equitable access to the internet, and digital inclusion influence ISP regulation. As the internet becomes an essential part of daily life, ensuring all individuals have fair and affordable access is a growing concern. Regulators ensure that ISPs contribute to bridging the digital divide, often requiring policies promoting investment in under-served areas.

This comparative research provides valuable insights into the complexities of ISP regulation across different legal and cultural landscapes. The findings contribute to a deeper understanding of global digital governance challenges and offer practical recommendations for enhancing ISP regulation in South Africa.

7.4 RESEARCH FINDINGS - SUMMARY

The culmination of this comparative legal study on the role and liability of ISPs across different jurisdictions has led to several key findings. These findings are instrumental in understanding the varying approaches to ISP regulation, the challenges encountered, and the potential pathways for enhancing regulatory frameworks in South Africa and beyond. The study underscored that there is no one-size-fits-all model for ISP regulation. Each jurisdiction has tailored its regulatory approach to suit its socio-political context, technological advancements, and legal traditions. South Africa, for instance, has established a regulatory regime that attempts to balance digital rights with national interests. Ireland's approach is marked by adherence to EU standards, emphasizing data protection and user rights. In contrast, China's model is characterized by stringent state control and extensive surveillance capabilities. Nigeria's evolving approach reveals efforts to strengthen its digital governance in the face of unique national challenges.

ISPs globally face a myriad of challenges. Common issues include ensuring data privacy, combatting cyber threats, managing content censorship, and balancing user freedom and legal compliance. These challenges are exacerbated by the rapid pace of technological change, which often outstrips the ability of regulatory frameworks to adapt. The research highlighted the need for ongoing legislative and policy updates to keep

pace with technological advancements and evolving cyber threats. The study revealed that legislative and judicial frameworks significantly impact ISP operations. Laws determine the scope of ISP responsibilities and liabilities, while judicial rulings clarify and sometimes extend these boundaries. There is a notable variation in how different jurisdictions interpret and enforce laws about ISPs. For example, judicial rulings in South Africa and Ireland have focused on balancing user rights with regulatory compliance, whereas, in China, court decisions have reinforced state control and censorship.

The comparative analysis provided valuable insights for South Africa. One key lesson is the importance of clear, enforceable regulations adaptable to technological changes. South Africa can benefit from looking at Ireland's alignment with EU standards, particularly in data protection and user privacy. The study also suggests that while stringent control, as seen in China, can be effective in content regulation, it may come at the cost of individual freedoms, a balance South Africa must navigate carefully. The research highlighted the importance of understanding global trends in Internet governance and applying these insights to local contexts. For South Africa, this means adopting best practices worldwide while ensuring regulations are tailored to local needs and conditions. This approach can help South Africa develop a more resilient, responsive, and user-centric ISP regulatory framework. ISPs are not just service providers but key players in the digital rights arena. The study indicated that ISPs are crucial in protecting user data, ensuring access to information, and safeguarding digital freedoms. In jurisdictions like Ireland and South Africa, ISPs are increasingly seen as partners in promoting digital rights, whereas in China, they are more instruments of state policy. Effective ISP regulation requires the involvement of multiple stakeholders, including government agencies, ISPs, civil society, and users. The research underscores the importance of collaborative approaches to policymaking, where different perspectives are considered to create balanced, effective regulations. The study also points to emerging issues, such as the impact of artificial intelligence, the Internet of Things, and 5G technology on ISP regulation. These developments present new challenges and opportunities for regulatory frameworks, requiring proactive and forward-looking policies.

7.5 RECOMMENDATIONS

a) Enhance Data Protection Legislation

Enhancing data protection legislation is critical in addressing the evolving challenges posed by new technologies, particularly in cloud computing and the Internet of Things (IoT). As the digital landscape transforms rapidly, ensuring that laws and regulations governing data protection are robust, comprehensive, and aligned with current and future technological advancements becomes increasingly essential.

Cloud computing has revolutionized data storage and access, offering flexibility, scalability, and efficiency. However, it also presents unique risks and challenges, especially regarding data privacy and security. Traditional data protection laws may not adequately address these challenges because they focus on more conventional data storage and management forms. Therefore, updating data protection legislation to include specific provisions for cloud computing is essential. This should involve setting clear standards for data encryption, access control, and regular security audits to ensure that data stored in the cloud is protected against unauthorized access and breaches.

Similarly, the proliferation of IoT devices has resulted in an exponential increase in data generated and collected. IoT devices often collect sensitive personal information, and the interconnected nature of these devices can make data more vulnerable to attacks. Updated legislation should address the unique nature of IoT data collection, processing, and storage. This includes mandating robust security measures for IoT devices and networks, such as secure authentication protocols and regular firmware updates to guard against vulnerabilities.

ISPs play a pivotal role in the digital ecosystem, often serving as gatekeepers to the internet and custodians of vast user data. As such, specific guidelines for ISPs on user data handling, storage, and security are crucial to enhanced data protection legislation. These guidelines should require ISPs to implement advanced security measures to

protect user data from cyber threats. This includes employing end-to-end encryption, secure data storage solutions, robust firewalls, and antivirus systems.

Furthermore, the legislation should mandate ISPs to be transparent in their data handling practices. This involves informing users about the type of data collected, the purposes of data collection, and the measures in place to protect their data. Users should also have easy-to-understand privacy policies and options to control their data usage and sharing.

Another important aspect of enhanced data protection legislation is ensuring compliance and enforcement. This can be achieved through regular audits of ISPs' data protection practices, strict penalties for non-compliance, and mechanisms for users to report violations of their data privacy rights. Additionally, ISPs should be required to report data breaches to relevant authorities promptly and affected users, along with clear communication on mitigating the impact. Given the internet's and digital technologies' global nature, international cooperation and harmonization of data protection standards are also crucial. This ensures that ISPs operating in multiple jurisdictions adhere to consistent data protection principles, providing users with uniform protection worldwide.

b) Regular Review of ISP Regulations

Implementing a mechanism for regularly reviewing and updating ISP regulations is essential to ensure that the regulatory framework adapts and remains effective amidst rapid technological advancements. As the digital landscape evolves, so do the challenges and opportunities within Internet service provision. Regularly reviewing ISP regulations is a matter of keeping up with technology and ensuring that these regulations continue to protect consumer interests, foster innovation, and address emerging threats in cyberspace.

The first step in this process is establishing a dedicated regulatory body or committee to monitor technological trends and their implications for ISPs. This body would periodically assess the current regulatory landscape and identify areas where updates or revisions

are needed to address new technological developments. Such a body should comprise technology, cybersecurity, law, and consumer rights experts to provide a well-rounded perspective on the needs and challenges in regulating ISPs.

Regular reviews should ensure that regulations are adaptable and flexible enough to accommodate new technologies and business models. For instance, the rise of decentralized technologies like blockchain, or the increasing use of artificial intelligence in network management and data analytics, presents new regulatory challenges and opportunities. The regulatory framework must be agile enough to respond to these changes without stifling innovation. Regular reviews should also consider the impact of technological advancements on consumer privacy and security. As ISPs increasingly become involved in processing and storing large volumes of personal data, regulations must ensure robust protection of this data against unauthorized access and breaches. This includes revisiting data protection policies, encryption standards, and requirements for ISPs to report data breaches.

Another important aspect is the interoperability and compatibility of regulations across jurisdictions. As ISPs often operate across national borders, regulatory reviews should consider international standards and practices to ensure harmonization and prevent regulatory fragmentation. This is crucial for maintaining a stable and consistent online environment and supporting the global nature of internet-based services. Public consultation should be an integral part of the regulatory review process. This involves engaging stakeholders, including ISPs, consumers, tech companies, and civil society, to gather input and feedback on proposed regulatory changes. Such consultations ensure that the regulations are balanced, addressing the needs and concerns of all parties involved. The mechanism for regular review should also include a process for rapid response to emerging threats, such as new forms of cyberattacks or exploitation of network vulnerabilities. This requires a proactive approach to regulation, where potential threats are anticipated and addressed before they become widespread.

c) Foster Multi-stakeholder Collaboration

Fostering multi-stakeholder collaboration is pivotal in developing comprehensive and balanced Internet governance strategies. This approach recognizes that effective regulation of ISPs and the broader digital landscape requires input from various sectors - government, ISPs, technology experts, and civil society. Each stakeholder brings unique perspectives and expertise for creating a holistic and practical regulatory framework. The government plays a crucial role in setting the legal and regulatory framework for ISPs. However, to ensure that these regulations are practical and forward-looking, the government must collaborate with those directly impacted by these policies and those with technical expertise. This includes ISPs, who understand the operational challenges and technological possibilities; technology experts, who can foresee emerging trends and potential risks; and civil society organisations, who can advocate for the rights and interests of consumers and the public.

A practical approach to foster this collaboration is establishing advisory councils or committees that bring together representatives from each group. These bodies can be tasked with specific goals, such as identifying emerging technological trends that require regulatory attention, proposing updates to data protection and privacy laws, or developing strategies to combat cybercrime. These councils should be able to conduct research, hold hearings, and gather various input. Their recommendations should then be seriously considered in the formulation of policies. This ensures that the regulations are based on theoretical understanding and grounded in practical realities and diverse perspectives.

For instance, in developing strategies to enhance cybersecurity, input from ISPs is crucial as they have firsthand experience with the types of cyber threats they encounter. At the same time, technology experts can provide insights into the latest cybersecurity technologies and best practices, while civil society groups can ensure that measures to enhance security do not unduly infringe on privacy and freedom of expression. Public-private partnerships can also be an essential element of multi-stakeholder collaboration. These partnerships can facilitate sharing resources, knowledge, and expertise between

the government and private sector, leading to more efficient and effective solutions to common Internet governance challenges.

Collaborative efforts should also extend to international cooperation, especially given the global nature of the internet. This can involve participation in international forums, alignment with global standards, and bilateral or multilateral agreements to address cross-border issues such as data privacy, cybercrime, and digital trade. Transparency and accountability are crucial in these multi-stakeholder collaborations. The processes and outcomes of these collaborative efforts should be open and accessible to the public to build trust and ensure legitimacy. Regular reporting, public consultations, and open forums can help achieve this transparency.

d) Improve Cybersecurity Standards

First and foremost, there is a need for a comprehensive set of cybersecurity strategies explicitly tailored to ISPs. These standards should be designed considering the unique challenges ISPs face, such as managing vast networks, handling large volumes of data, and being at the forefront of emerging cyber threats. The standards should encompass various aspects of cybersecurity, including network security, data encryption, access control, threat detection, and incident response.

Mandating regular security audits is critical to ensuring ISPs comply with these cybersecurity standards. These audits should be conducted by independent, certified professionals who can objectively assess the ISPs' security posture. The audits should assess compliance with established standards and evaluate the ISPs' ability to respond to and recover from cyber incidents. This includes examining their incident response plans, backup strategies, and disaster recovery protocols.

In addition to audits, periodic compliance checks should be implemented. These checks, conducted by regulatory authorities, can ensure that ISPs consistently adhere to the required cybersecurity standards. They can also help identify areas where ISPs need additional support or guidance to meet the standards.

These cybersecurity standards should be regularly updated to keep pace with the rapidly evolving cyber threat landscape. This requires a dynamic approach where feedback from ISPs, insights from cybersecurity experts, and lessons learned from recent cyber incidents are continuously incorporated into the standards. Collaboration with international cybersecurity agencies and standard-setting bodies can help stay updated with global best practices and emerging threats.

Educating and training ISP personnel in cybersecurity is another vital aspect. ISPs should be encouraged to invest in regular training programs for their employees to ensure they know the latest cyber threats and best practices in cybersecurity. This includes training in identifying potential threats, handling security breaches, and maintaining customer privacy.

Moreover, ISPs should be encouraged to adopt a proactive approach to cybersecurity. Instead of merely reacting to incidents, ISPs should invest in advanced threat detection and predictive analytics tools to identify potential threats before they materialize. This proactive stance not only protects the ISPs but also contributes to the overall security of the digital ecosystem. Enforcement mechanisms are crucial for ensuring compliance with cybersecurity standards. Regulatory authorities should be able to impose penalties on ISPs that fail to meet the required standards. However, these enforcement measures should be balanced with support mechanisms, such as providing ISPs access to cybersecurity resources, tools, and expertise.

e) Promote Digital Literacy and Inclusion

Promoting digital literacy and inclusion is integral to fostering a safe and inclusive digital environment. In today's age, all population segments must be equipped with the skills and knowledge to use the internet safely and effectively. Additionally, addressing the digital divide is crucial to ensure equitable access to internet services, enabling everyone, irrespective of their socio-economic background, to benefit from the digital revolution.

To achieve this, the development and implementation of comprehensive initiatives to enhance digital literacy are necessary. These initiatives should be multifaceted and designed to reach diverse populations, including those in rural areas, older people, and socio-economically disadvantaged groups. The curriculum for digital literacy programmes should cover basic computer skills, internet safety, understanding of digital rights and privacy, and awareness of online misinformation and cyber threats.

One effective approach is integrating digital literacy into the education system at all levels, from primary schools to higher education. This ensures that young people grow up as digital natives, equipped with the necessary skills to navigate the digital world; for adults and older people, community-based training programs can be established, possibly in collaboration with local libraries, community centres, and non-profit organisations. These programs should be tailored to adults' specific needs and learning styles, focusing on practical skills to enhance their daily lives and work. Beyond just literacy, there is a need to bridge the digital divide. This involves ensuring that all individuals can access affordable and reliable internet services. Governments should invest in infrastructure development in collaboration with ISPs and private sector partners, especially in underserved and rural areas. Subsidies or affordable internet plans for low-income households can also be considered to make internet access more inclusive. Public awareness campaigns are another key component of promoting digital literacy and inclusion. These campaigns can highlight the importance of digital skills in the modern world, the risks associated with the digital divide, and the resources available for individuals to improve their digital literacy. Traditional and social media can play a significant role in disseminating these messages effectively.

Innovation in technology solutions can also help in bridging the digital literacy gap. For instance, developing user-friendly and accessible technologies can make it easier for older people and people with disabilities to access and use digital services. Mobile applications that provide easy-to-understand tutorials and guidance on using digital tools can benefit those new to the internet. Furthermore, partnerships between the government, private sector, civil society, and educational institutions are crucial for

successful digital literacy and inclusion initiatives. These partnerships can leverage the strengths and resources of different stakeholders to develop more comprehensive and sustainable programs.

f) Content Regulation and Freedom of Expression

Establishing clear, transparent, and fair guidelines for content moderation by ISPs is essential to balance the imperative to filter harmful content with preserving freedom of expression. This balance is critical in a digital environment where the internet plays a significant role in disseminating information and ideas. The approach to content regulation must protect users from harmful or illegal content while respecting their right to free speech and access to information.

To achieve this, it is necessary to define what constitutes 'harmful content' precisely and clearly. This definition should be based on objective criteria and align with international human rights standards. Content that incites violence propagates hate speech, violates privacy rights, or constitutes child exploitation, for instance, should be universally recognized as harmful. However, care must be taken to ensure that the definition does not become overly broad or subjective, leading to unnecessary censorship or infringement on individual rights. ISPs should be provided with transparent guidelines on how to moderate content. These guidelines should be developed through a multi-stakeholder process involving government representatives, ISPs, civil society, legal experts, and other relevant parties. This collaborative approach ensures that the guidelines are well-rounded and practical and consider diverse perspectives.

Transparency in content moderation processes is crucial. ISPs should disclose their content moderation policies and procedures to their users. This transparency helps build trust and understanding among users about how and why certain content may be moderated. It also provides a basis for accountability if ISPs are perceived to be overstepping their bounds. There should be a mechanism for appeal and redress for users who believe their content has been unfairly moderated. This mechanism ensures that users can challenge decisions that infringe on their freedom of expression. The

process should be straightforward, accessible, and timely to ensure effective redress. In addition to self-regulation by ISPs, independent oversight can be established to ensure that ISPs adhere to the established guidelines. This oversight body can review content moderation decisions, provide guidance, and ensure that ISPs' practices align with legal and ethical standards.

Freedom of expression is a fundamental right, and its preservation in the digital realm is crucial. However, it is equally important to recognize that this freedom comes with responsibilities. ISPs, while respecting freedom of expression, must also take proactive steps to prevent their platforms from being used to spread harmful content. This includes investing in technology and human resources to identify and mitigate such content effectively. The balance between filtering harmful content and preserving freedom of expression is delicate and complex. It requires continuous dialogue, evaluation, and adjustment of policies and practices. By establishing clear guidelines, ensuring transparency and accountability, and fostering a culture of respect for individual rights, it is possible to create a digital environment that is both safe and free, allowing for the robust exchange of ideas and information.

g) Strengthen International Collaboration

Strengthening international collaboration is pivotal in developing uniform standards for data protection, cybersecurity, and internet governance. In an increasingly interconnected digital world, threats and challenges in cyberspace do not recognize national borders, making international cooperation beneficial and necessary for effective regulation and enforcement.

Engaging in international collaboration involves participating actively in global forums and discussions on Internet governance, data protection, and cybersecurity. Such participation allows for exchanging best practices, insights, and experiences with other nations, fostering a comprehensive understanding of global digital challenges. Developing uniform standards for data protection is critical, as the varying regulations across countries can create complexities, especially for ISPs operating in multiple

jurisdictions. A coordinated approach can help establish global data protection standards that respect individual privacy rights while recognizing the necessity of data flow for economic development. This approach should be inclusive, considering the perspectives of developing and developed countries to ensure that the standards are equitable and universally applicable.

In cybersecurity, international collaboration is essential due to the borderless nature of cyber threats. Nations can share intelligence about emerging threats, coordinate responses to large-scale cyber incidents, and develop joint strategies to enhance global cyber resilience. Collaborative efforts might include joint exercises, research and development initiatives, and sharing best practices for critical infrastructure protection.

Internet governance, a multifaceted issue encompassing various aspects, from freedom of expression to economic transactions, requires a coordinated global approach. International collaboration can help develop a consensus on key issues like net neutrality, content regulation, and the management of Internet resources. Such a consensus is vital for maintaining the Internet as an open, secure, and reliable resource accessible to all. Furthermore, this collaboration can extend to law enforcement and judicial cooperation, especially in combating cybercrime. Cross-border legal frameworks and extradition treaties can be established or strengthened to prosecute cyber-crimes effectively. This requires harmonizing legal definitions and penalties for cyber offences and establishing protocols for information sharing and joint investigations.

Engaging with international organisations such as the United Nations, the International Telecommunication Union, the Internet Governance Forum, and regional bodies like the European Union, ASEAN, or the African Union can be effective. These platforms provide opportunities to influence global internet policy and align national regulations with international standards. It is also essential to recognize the dynamic nature of technology and cyberspace. International collaboration should be flexible and adaptable to rapidly evolving digital landscapes. Regular dialogues, conferences, and summits can be organized to keep up with these changes and update standards and policies accordingly.

h) Encourage Ethical ISP Practices

Encouraging ethical practices among ISPs is vital in ensuring they operate in a manner that respects user privacy, protects data, and manages content responsibly. Developing a comprehensive code of ethics for ISPs is a guideline to uphold these standards and fosters trust between ISPs, their users, and regulatory bodies.

The code of ethics should encompass critical principles such as transparency, accountability, fairness, and respect for user rights. Transparency in ISP operations involves clear communication with users about data collection, processing, and sharing practices. ISPs should inform users about how their data is used and the measures taken to protect it. This transparency builds user trust and helps ISPs avoid data misuse or unauthorized access conflicts.

Accountability is another critical aspect. ISPs should be accountable for their actions, especially regarding data breaches or misuse of user information. The code of ethics should outline the procedures for reporting data breaches, including timely notification to affected users and relevant authorities. It should also specify the consequences of ethical violations, ensuring ISPs are held responsible for their actions.

Fairness in content management is essential. ISPs often find themselves in a position where they need to balance content regulation with freedom of expression. The code of ethics should provide guidelines for content moderation that are fair, non-discriminatory, and respectful of free speech. It should outline procedures for handling controversial content, ensuring decisions are made objectively based on clearly defined criteria. Respect for user privacy and data protection is a cornerstone of ethical ISP practices. The code should emphasize the importance of safeguarding user data and outline the standards for privacy protection. This includes encryption, ensuring secure data storage, and implementing strong access controls. ISPs should be encouraged to adopt privacy-by-design approaches, integrating data protection measures into their service offerings.

The code should also address the ethical use of new AI and machine learning technologies in ISP operations. These technologies can significantly impact user privacy and data security. Guidelines should be established for the responsible deployment of these technologies, ensuring they are used transparently and respect user rights. To ensure compliance, the code of ethics should be enforced through a combination of self-regulation, industry oversight, and regulatory frameworks. ISPs should be encouraged to internalize these ethical standards, incorporating them into their corporate policies and operational procedures. Regular training and awareness programs about ethical practices and data protection are essential for ISP staff.

i) Develop ISP Liability Framework

Developing a clear and well-defined legal liability framework for ISPs is essential to ensure that the responsibilities and liabilities of ISPs regarding the content they host and transmit are fair, proportionate, and transparent. This framework should aim to balance the ISPs' role in providing access to information with the need to control illegal and harmful content without placing undue burdens on the ISPs or stifling freedom of expression and innovation. The framework should start by delineating the types of liabilities ISPs can face. This includes liability for hosting illegal content, such as copyright-infringing materials, defamatory statements, or content that promotes terrorism or other criminal activities. The framework should clarify the circumstances under which an ISP becomes aware of such content and its obligations in response. This could include mechanisms for notice and takedown procedures, where ISPs must remove content upon receiving a valid notification.

It is also crucial to differentiate between content types and the corresponding liability level. For instance, the liability associated with knowingly hosting illegal content should be distinct from inadvertent hosting. The framework should guide how to handle grey areas where the legality of content is not clear-cut. In these cases, ISPs should not be expected to act as judges of content legality but should have clear procedures involving judicial oversight. Another aspect to consider is the protection of ISPs from liability for

user-generated content if they comply with certain conditions, such as following proper procedures upon notification of illegal content. This approach, often called “safe harbour” provisions, encourages ISPs to act responsibly without fearing constant legal challenges.

The framework should also address the challenges posed by new technologies like encryption and peer-to-peer networks. These technologies can complicate the ability of ISPs to monitor and control the content passing through their networks. The liability framework should consider the technical feasibility and compliance burden on ISPs. Transparency in the process of content moderation and takedown is also vital. ISPs should be required to publish transparency reports detailing requests for content removal, compliance rates, and any challenges faced. This transparency helps build trust among users and provides insights into the ISPs' content moderation practices.

Furthermore, the liability framework should encourage ISPs to implement best practices in content moderation, such as employing a diverse team of moderators, providing adequate training, and using a combination of automated and human review processes. The goal is to ensure that content moderation is unbiased and respects users' rights. To ensure the effectiveness of the liability framework, it should be developed in consultation with a wide range of stakeholders, including ISPs, legal experts, civil society organisations, and the public. This inclusive approach ensures that the framework is balanced and considers different perspectives.

j) Support Innovation and Competition

Creating a supportive environment for innovation and competition among ISPs is vital for advancing technology and providing high-quality Internet services. This approach can lead to more consumer choices, better service quality, and lower prices, benefiting the entire digital ecosystem. To foster innovation and competition, it is essential to establish a regulatory framework that is conducive to the entry of new ISPs into the market. This can be achieved by reducing bureaucratic hurdles and providing a level playing field for all players, regardless of size. Simplifying licensing processes, offering

transparent and fair criteria for market entry, and minimizing unnecessary regulatory burdens are crucial steps in this direction. Encouraging competition also ensures that existing market players do not engage in anti-competitive practices. Regulatory authorities should closely monitor and prevent activities such as price-fixing, monopolistic practices, or unfair restrictions on new entrants. Establishing an independent regulatory body with the power to enforce competition laws and address complaints can help maintain a healthy competitive environment.

Supporting innovation requires investment in research and development (R&D) within the ISP sector. Governments and industry bodies can play a significant role by providing funding, tax incentives, and other support for R&D activities. Collaborations between ISPs, academic institutions, and technology companies can also drive innovation, developing new technologies, services, and business models. Ensuring that ISPs have access to necessary resources, such as spectrum and infrastructure, is equally important. Efficient and fair spectrum allocation and policies that encourage infrastructure sharing can reduce costs and barriers to entry for new ISPs. This approach promotes competition and accelerates the deployment of advanced technologies like 5G.

Another aspect of supporting innovation and competition is to embrace and adapt to new technological developments. Regulatory frameworks should be flexible enough to accommodate emerging technologies and business models without stifling them with outdated rules. This flexibility ensures ISPs can experiment with and adopt new technologies like blockchain, IoT, and cloud computing, leading to more innovative consumer services.

Fostering a culture of customer-centric innovation is also crucial. ISPs should be encouraged to improve customer experience through better service quality, innovative product offerings, or enhanced customer support. Regulatory frameworks can support this by setting high standards for service quality and customer care. In addition, promoting digital literacy and consumer awareness can create a more informed

customer base that demands better and more innovative services. Educated consumers are more likely to switch providers in search of better service, thereby driving competition and innovation in the ISP market.

7.6 CONCLUSION

In conclusion, the research goals have been met in that the researcher has investigated, discovered, and described the role and liability of ISPs in South Africa and comparative jurisdictions using a critical and comparative appraisal, which has satisfied the research questions posed at the outset. The researcher has also utilized the knowledge acquired from the findings of this study in formulating recommendations that can assist in effectively strengthening the role and liability of ISPs involved in providing services in South Africa.

In South Africa, the legal and regulatory framework governing ISPs primarily focuses on deterring cybercrime, protecting user privacy, and upholding freedom of expression. However, the effectiveness of these laws in achieving their intended objectives is mixed. While robust mechanisms exist for data protection and cybercrime deterrence, challenges persist in balancing these objectives with the need to maintain freedom of expression and innovation. ISPs in South Africa face the ongoing task of aligning with these regulations while responding to technological advancements and market demands. The study's examination of China, Ireland, and Nigeria revealed distinct approaches to ISP regulation. China’s stringent control over ISPs, primarily for content censorship and surveillance, contrasts sharply with the more liberal and privacy-focused approaches observed in Ireland and Nigeria. Ireland’s alignment with EU standards, especially regarding data protection and user rights, offers valuable lessons in balancing regulation with promoting digital freedoms. Nigeria’s evolving ISP framework, facing challenges like South Africa, shows efforts towards strengthening cyber laws and encouraging digital inclusion. In South Africa, the legislative framework, though comprehensive, faces implementation challenges, particularly in enforcing cybercrime laws and ensuring ISPs comply with data protection regulations. The comparative

analysis suggests that adopting best practices from other jurisdictions, such as Ireland's robust data protection laws or Nigeria's initiatives for digital inclusion, could enhance the effectiveness of South African ISP regulations.

ISP regulations have far-reaching implications for various stakeholders. Consumers demand reliable and secure internet services, ISPs seek operational clarity and fair competition, and the government aims to protect national interests and promote digital advancement. Balancing these interests is complex, as seen in the varied approaches of the studied jurisdictions. The need for multi-stakeholder collaboration emerges as a crucial element in developing effective Internet governance strategies.

Technological advancements present both opportunities and challenges for ISP regulation. The rapid evolution of digital technologies, such as IoT and AI, requires adaptable and forward-looking regulatory frameworks. Ethical considerations, particularly regarding user privacy and freedom of expression, remain at the forefront of ISP regulation debates. The study underscores the importance of continuous regulatory review and adaptation to technological changes.

Based on these findings, the study proposes several recommendations for enhancing ISP regulation in South Africa. These include updating data protection laws, fostering multi-stakeholder collaboration, improving cybersecurity standards, promoting digital literacy and inclusion, and strengthening international cooperation.

BIBLIOGRAPHY

Access Now. (2023, June 1). *Internet Shutdowns in 2023: A Mid-Year #KeepItOn Update*. Retrieved from Access Now: https://www.accessnow.org

Adebayo, I. (2017, March 8). *Nigeria losses due to Cyber Crime: Annual Review*. Retrieved from Daily Post: http://dailypost.ng/2017/03/08/nigeria-losses-n127b-annually-cyber-crimebuhariper centE2percent80percent8E/

African Union. (2020, June 12). *African Internet Exchange Systems (AXIS) Project Overview*. Retrieved from African Union: https://au.int/en/african-internet-exchange-system-axis-project-overview

African Union. (2020, October 9). *Agenda 63: The Africa We Want*. Retrieved from African Union: https://au.int/en/agenda2063/overview

African Union. (2020, May 18). *The Digital Transformation Strategy (2020-2030)*. Retrieved from African Union: https://au.int/en/documents/20200518/digital-transformation-strategy-africa-2020-2030

Aon South Africa. (2023, November 11). *Cybercrimes Act Report 2023*. Retrieved from Aon: https://www.aon.co.za

Arpanet. (2023, November 23). *Definition, history & significance*. Retrieved from Study.com: https://study.com/academy/lesson/arpanet-definition-history-quiz.html#:~:text=ARPANET%20was%20invented%20by%20a,ARPANET%20was%20born%20in%201969.

Bagraim, J. (2010). Multiple affective commitments and salient outcomes: the impossible case of information technology knowledge workers. *Electronic Journal of Information Systems Evaluation*, 97-106.

Beaumont, P. (2011, February 25). *The truth about Twitter, Facebook and the uprisings in the Arab World*. Retrieved from The Guardian: https://www.theguardian.com/world/2011/feb/25/twitter-facebook-uprisings arab-libya

BRM. (2021, June 23). *Interpretivism (intepretivist) Research Philosophy*. Retrieved from Business Research Methodology: https://research-methodology.net/research-philosophy/interpretivism/

Buckley, C., & Ramzy, A. (2014, October 1). *Hong Kong protests are leaderless but orderly*. Retrieved from The New York Times: https://www.nytimes.com/2014/10/01/world/asia/in-hong-kong-clean-and-polite-but-a protest-nonetheless.html

Budapest Convention on Cybercrime. (n.d.).

Chen, T. P., Law, F., & Purnell, N. (2014, January 28). *Apps speed up and often muddle Hong Kong protestors' messages*. Retrieved from The Wall Street Journal: https://www.wsj.com/articles/whatsapp-key-to quickly-rallying-protesters-in-hong-kong-but-groups-struggle-to-stay-on-message 1412878808

Citizens Information. (2023, February 1). *Overview of the General Data Protection Regulation*. Retrieved from Citizens Information: https://www.citizensinformation.ie/en/government-in-ireland/data-protection/overview-of-general-data-protection-regulation/

Comninos, M. (2012, June 12). *Intermediary liability in South Africa*. Retrieved from APC: https://www.apc.org/en/system/files/Intermediary_Liability_in_South_Africa-

Constitution of the Federal Republic of Nigeria. (n.d.).

Constitution of the Republic of South Africa, 1996. (n.d.).

Consumer Protection Act 68 of 2008. (n.d.).

Convention on Cyber Security and Personal Data Protection. (n.d.). African Union.

Council of Europe. (2023, June 23). *The International Covenant on Civil and Political Rights*. Retrieved from COE: https://www.coe.int/en/web/compass/the-international-covenant-on-civil-and-political-rights

Cybercrimes Act 19 of 2020. (n.d.).

Cybersecurity Law of the People's Republic of China. (2017).

Dann, G. E., & Haddow, N. (2008). Just doing business or doing just business: Google, Microsoft, Yahoo and the business of censoring China's Internet. *Journal of Business Ethics*, 219-234.

Darrynn, N. (2015, December 19). *Bandwidth in South Africa explained*. Retrieved from Optimus: http://www.optimus01.co.za/bandwidth-in south-africa-explained/

DataReportal. (2023, January 9). *Digital 2023: Global Overview Report*. Retrieved from DataReportal: https://www.datareportal.com

Delfi v Estonia, 64569/09 (European Court of Human Rights October 2013).

DemandSage. (2024, January 9). *Internet User Statistics in 2014*. Retrieved from DemandSage: www.demandsage.com

Department of Enterprise, Trade and Employment. (2020, January 22). *Digital Single Market*. Retrieved from Enterprise.Gov: https://enterprise.gov.ie/en/what-we-do/the-business-environment/digital-single-market/

Deutch, K. (2001). Comparative criminal justice systems. In E. Fairchild, & H. R. Dammer, *Comparative criminal justice systems* (pp. 4-19). California: Wadsworth/Thomas Learning.

Dharmawan, N. S., Kasih, D. D., & Stiawan, D. (2019). Personal data protection and liability of internet service providers: a comparative approach. *Internet Journal of Electrical and Computer Engineering, 9*(4), 3175-3184.

Dongjin Consulting. (2019, December 25). *Provisions on Governance of the Network Information Content*. Retrieved from Dongjin Consulting: http://en.shanghaiinvest.com/information-center/newsletters/item/333-provisions-on-governance-of-the-network-information-content

Duffett, R., Petrosanu, D. M., Negricea, I. C., & Edu, T. (2019). Effect of YouTube Marketing Communication on Converting Brand LInking into Preference among Millenials Regarding Brands. *Sustainability, 11*(3), 600-645.

ECTA Cryptography Regulations No. 8418. (2006, March 10).

Electronic Communications and Transactions Act 25 of 2002. (n.d.).

Electronic Communications and Transactions Amendment Act, No. 1 of 2014. (n.d.).

Eloff, D. J. (2020). A comparative inquiry into internet neutrality in South Africa. *Unpublished doctoral dissertation*. University of Pretoria.

Eltantawy, N., & Wiest, J. (2011). Social Media in the Egyptian Revolution: Reconsidering Resource Mobilization Theory. *International Journal of Communication*, 1207-1245.

European Commission. (2023, June 17). *Implementation of the NIS Directive in Ireland*. Retrieved from European Commission: https://digital-strategy.ec.europa.eu/en/policies/nis-directive-ireland

European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations. (n.d.).

European Union (Consumer Information, Cancellation and Other Rights) Regulations. (n.d.).

Farelo, M., & Morris, C. (2006, June 19). *The status of e-government in South Africa*. Retrieved from Research Space: “The status of e-government in South Africa” http://researchspace.csir.co.za/dspace/bitstream/10204/966/1/Farelo_2006_D.pdf

Fernandez Nieto, B. (2022, September 9). The role of Internet service providers in protecting digital rights. *Unpublished doctoral thesis*. University of Glasgow.

Fernando , R. (2022, March 21). The liability of Internet service providers for copyright infringement in Sri Lanka: A comparative analysis. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4080952

Flyverbom, M., Deibert, R., & Matten, D. (2019). The governance of digital technology, big data, and the Internet: new roles and responsibilities for business. *Business and Society, 58*(1), 3-19.

Fortinet. (2020, July 22). *What is cryptography*? Retrieved from Fortinet: https://www.fortinet.com/resources/cyberglossary/what-is-cryptography

Freedom of Information Act. (2011).

Gallagher, R. (2018, August 1). *Google plans to launch a censored search engine in China, leaked documents reveal*. Retrieved from The Intercept: https://theintercept.com/2018/08/01/google-china-search-engine-censorship/

General Data Protection Regulation. (n.d.). European Union.

General Data Protection Regulation (Ireland). (n.d.).

Giftwrap Trading (Pty) Ltd v Vodacom (Pty) Ltd and Others (1009/2020) [2023] ZASCA 47.

Gillis, A. S. (2022, February 1). *ISP (Internet Service Provider)*. Retrieved from TechTarget: https://www.techtarget.com/whatis/definition/ISP-Internet-service-provider

Gray Group International. (2023, November 12). *Globalization: Dissecting the Global Interconnectedness Maze*. Retrieved from Gray Group International: https://www.graygroupintl.com/blog/globalization

Greenleaf, G. (2021). China's completed Personal Information Protection Law: rights plus cyber security. *UNSW Law Research Paper*, 21-91.

Guo, E. (2023, December 12). *Inside the decades-long fight over Yahoo's misdeeds in China*. Retrieved from MIT Technology Review: https://www.technologyreview.com/2023/12/12/1084990/yahoo-china-dissident-yahoo-human-rights-fund/#:~:text=In%202002%2C%20Yahoo%2C%20whose%20CEO,end%20of%20one%2Dparty%20rule.

H v W 2013 2 SA 530 (GSJ) .

Haas, B. (2017, July 19). *China blocks WhatsApp services as censors tighten grip on internet*. Retrieved from The Guardian: https://www.theguardian.com/technology/2017/jul/19/china-blocks-whatsapp services-as-censors-tighten-grip-on-internet

Hempel, J. (2016, January 1). *Social Media made the Arab Spring, but could'nt save it*. Retrieved from Wired: https://www.wired.com/2016/01/social-media-made-the-arab-spring-but-couldnt-save-it/

Hu, H. L. (2011). The political economy of governing ISPs in China: perspectives of net neutrality and vertical integration. *The China Quarterly*(207), 2011.

Ifonlaja, O. (2023, August 7). Legal Framework for the Regulation of Internet Service Providers in Nigeria. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4533451

Independent Communications Authority of South Africa Act 13 of 2000. (n.d.).

Interim Provisions Governing Management of Computer Information Networks in the People's Republic of China Connecting to the International Network. (1996).

International Telecommunicaiton Union. (2023, November 11). *About the ITU*. Retrieved from International Telecommunications Union (ITU): https://www.itu.int/en/about/Pages/default.aspx

International Telecommunication Union. (2023, January 21). *Facts and Figures 2023 - Internet Use*. Retrieved from ITU: https://www.itu.int

Internet Live Stats. (2016, January 19). *Internet Users Worldwide*. Retrieved from Internet Live Stats: https://www.internetlivestats.com/internet-users/

Internet Service Providers Association. (2016, March 12). *Code of Conduct*. Retrieved from ISPA: http://ispa.org.za/code-of-conduct/request-atake-down/

Internet Society of China. (2016, November 24). *Introduction*. Retrieved from ISC: https://www.isc.org.cn/en

Internet World Stats. (2015, August 22). *African Internet Use and Statistics*. Retrieved from Internet World Stats: http://www.internetworldstats.com/stats1.htm

Internet World Stats. (2020, March 1). *Internet Penetration in Africa 2020 - Q1 - March*. Retrieved from Internet World Stats: Usage and Population Statistics: https://www.internetworldstats.com/stats1.htm

Ireland: Electronic Communications Networks and Services Regulation. (n.d.).

Ireland Broadcasting Act 2009. (n.d.).

Ireland Child Trafficking and Pornography Act. (1998).

Ireland Copyright and Related Rights Act. (2000).

Ireland Criminal Justice (Money Laundering and Terrorist Financing) Act. (2010).

Ireland Criminal Justice (Offences Relating to Information Systems) Act. (2017).

Ireland Data Protection Act. (2018).

Ireland Defamation Act. (2009).

Ireland. (1945). Bunreacht na hÉireann = Constitution of Ireland. Dublin :Oifig an tSoláthair,. (1945).

ISPA. (2016, January 24). *ISPA Super Teacher of the Year is today South Africa's foremost ICT in education competition for teachers*. Retrieved from ISPA: http://ispa.org.za/press-release/ispa-superteacher-of-the-year-is-today-south africas-foremost-ict-in-education-competition-for-teachers/

ISS Africa. (September 14 2022). *South Africa Lays Down the Law on Cybercrime*. Retrieved from ISS Africa: https://www.issafrica.org

Jemilohun, B. (2019). Liability of internet service providers under Nigerian Law. *African Journal of Legal Studies, 11*(4), 352-370.

Jouanjan, O. (2009). Freedom of expression in the Federal Republic of Germany. *Indiana Law Review*, 867-883.

Junda, Z. A. (2021). Liability of internet service providers to control online copyright infringement under Ethiopian copyright law. *Unpublished Doctoral Dissertation*. Haramaya University.

Ketler Investments CC t/a Ketler Presentations v Internet Service Provider All SA 566 (GSJ).

Kumar, R. (2019). *Research Methodology: A step-by-step guide for beginners.* New York: Sage.

Lee, J. A., & Liu, W. (2013). Searching for Internet freedom in China: a case study on Google's China Experience. *Cardoza Arts & Entertainment*, 405-434.

Lembani, R., Gunter, A., Breines, M., & Dalu, M. T. (2020). The same course, different access: the digital divide between urban and rural distance education students in South Africa. *Journal of Geography in Higher Education, 44*(1), 70-84.

Lenaerts, K. (2015). The case law of the ECJ and the internet. *ELTE Law Journal*, 9-25.

Levinsohn, K. (2017, January 23). *The real cost of uncapped ADSL in South Africa*. Retrieved from BandwidthBlog: http://www.bandwidthblog.com/2013/03/20/the-real-cost-of-uncapped-adsl-in-sa/

Lewis, J. A. (2010). Sovereignty and the Role of Government in Cyberspace. *Brown Journal of World Affairs*, 55-65.

Major, R. K. (2021). A Service Recovery Model for the Mobile Internet Service Provider Industry. *Unpublished Doctoral Dissertation*. North-West University.

Media Mags. (2017, May 1). *SA Ranks World's Third Highest Cybercrime Victims*. Retrieved from Business Media Mags: http://businessmediamags.co.za/sa-ranks-worlds-third-highest-cybercrime-victims-2/

Mhlanga, D., & Moloi, T. (2020). COVID-19 and the digital transformation of education: what are we learning on 4IR in South Africa? *Education Sciences*, 180-193.

Mishra, S. B., & Alok, S. (2022). *Handbook of Research Methodology.* London: Bloomsbury.

Mphidi, H. (2008). Digital divide and e-governance in South Africa. *Research, Innovation and Partnerships Tshwane University of Technology*, pp. 1-18.

Mpungose, C. B. (2020). Emergent Transition from Face-to-Face to Online Learning in a Southern African University in the Context of the Coronavirus Pandemic. *Humanities and Social Science Communications, 7*(1), 1-9.

Mupangavanhu, Y., & Kerchhoff, D. (2023). Online deceptive advertising and consumer protection in South Africa - the law and its shortcomings. *De Jure Law Journal, 56*(1), Online.

Murphy, N. (2016, June 12). *History of the Irish Internet*. Retrieved from InternetHistory: http://www.internethistory.ie/

NASDAQ. (2023, June 13). *Internet usage within developing markets has soared*. Retrieved from Nasdaq: https://www.nasdaq.com/articles/internet-usage-within-developing-markets-has-soared

National Media v Joost 1996 3 SA 262 (SCA). .

National People's Congress. (2005, September 22). *Decision of the Standing Committee of the National People's Congress on Preserving Computer Network Security*. Retrieved from English.Gov: http://english.gov.cn/laws/2005–09/22/content_68771.htm

Newman, M., & Gough, D. (2020). Systematic reviews in educational research: methodology, perspectives and application. *Educational Research Journal*, 3-22.

Nigeria Cybercrimes Act. (2015).

Nigeria Telecommunications Sector Reform Act. (1992).

Nigerian Anti-Terrorism Act. (2011).

Nigerian Child Rights Act. (2003).

Nigerian Communication Act 2003. (n.d.).

Nigerian Communications Act. (2003).

Nigerian Consumer Protection Framework. (n.d.).

Nigerian Copyright Act. (1988).

Nigerian Data Protection Regulation. (2019).

Nigerian Data Protection Regulation. (2019).

Nigerian Economic and Financial Crimes Commission (Establishment) Act. (2004).

Nigerian Information Technology Development Agency Act. (2007).

Norton Life Lock. (2021, October 1). *The Norton Cyber Safety Insights Report*. Retrieved from Norton Life Lock: https://www.nortonlifelock.com/us/en/newsroom/press-kits/2021-norton-cyber-safety-insights-report/

Nyinevi, C., & Ayalew, Y. E. (2022). Let the NetWork': The Role of African Sub-Regional Courts in Protecting Internet Access and Human Rights in the Digital Environment. *African Journal of International Economic Law*, 99-119.

Okai-Ugbaje, S., Ardzejewska, K., & Imran, A. (2020). Readiness, Roles, and Responsibilities of Stakeholders for Sustainable Mobile Learning Adoption in Higher Education. *Education Sciences, 10*(3), 43-53.

Open Net Initiative. (2019, January 14). *Country Profile: China"*. Retrieved from OpenNet: https://opennet.net/countries/china

Pandey, P., & Pandey, M. M. (2021). *Research methodology, tools and techniques.* London: Bridge Center.

People's Republic of China: Administration of Internet Electronic Messaging. (2000).

People's Republic of China: Decision of the Standing Committee of the National People's Congress on Preserving Computer Network Security. (n.d.).

People's Republic of China: Measures on Internet Information Services. (n.d.).

Peoples Republic of China: Personal Information Protection Law. (2021).

People's Republic of China: Provisions on the Governance of the Online Information Content. (2019).

People's Republic of China: Public Pledge of Self-Regulation and Professional Ethics for China's Internet Industry. (2000).

People's Republic of China: State Council Order 292. (n.d.).

PEW Research Centre. (2016, January 21). *Emerging nations embrace the internet and mobile technology*. Retrieved from Pew Global: http://www.pewglobal.org/2014/02/13/emerging-nations-embrace-internet-technology

Poushte, J. (2016). *Smartphone ownership and internet usage continue to climb in emerging economies, but advanced economies still have higher rates of technology use.* Washington DC: PEW Research Centre.

Promotion of Access to Information Act 2 of 2000. (n.d.).

Quinlan, C., Babin, B., Carr, J., & Griffin, M. (2019). *Business Research Methods.* Boston: Cengage.

Radebe, J. (2015, November 2). *Gauteng e-Government and ICT Summit*. Retrieved from Gov.Za: http://www.gov.za/speeches/minister-jeff-radebe-gauteng-e-government-and-ict-summit

RAND. (2023, September 1). *The future of Cybercrime in light of technological developments*. Retrieved from Rand: https://www.rand.org

Reddick, C. G., Enriquez, R., Harris, R. J., & Sharma, B. (2020, October 29). Determinants of Broadband Access and Affordability: An analysis of a community survey on the digital divide. *Cities*.

Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002. (n.d.).

SABAM v Netlog NV, C-360/10 (Court of Justice of the European Union February 16, 2012).

Scarlet Extended SA v Societe Belge des Auteurs, Compositeurs et Editeurs SCRL (SABAM), (C-70/10) [2011] (ECR November 24, 2011).

Sheehy, K. (2017, January 18). *Know your internet options: DSL, Cable, Fiber Optic*. Retrieved from Nerd Wallet: https://www.nerdwallet.com/article/utilities/understanding-difference-dsl-cable-fiberoptic-internet-service

Simonite, T. (2019, June 3). *US Companies help censor the internet in China, too*. Retrieved from Wired: https://www.wired.com/story/us-companies-help-censor-internet-china/

Sorbán, K. (2019). The Role of Internet Intermediaries in Combatting Cybercrime: Organisation and Liabilities. *Central and Eastern European eDem and eGov Days*, 19-31.

South African Info. (2016, November 14). *South African consumer service bodies*. Retrieved from South Africa Info: http://www.southafrica.info/services/consumer/consumer.htm#.V4EJueR7VEA

Stanford University. (2019, June 12). *Free speech vs Maintaining social cohesion: a closer look at different policies*. Retrieved from Stanford Edu:

https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/FreeExpressionVsSocialCohesion/china_policy.html

Statista. (2023, October 31). *Number of internet users and social media users worldwide as of October 2023*. Retrieved from Statists: https://www.statista.com/statistics/617136/digital-population-worldwide/

TechArchives. (2019, June 1). *How the internet came to Ireland 1987-97*. Retrieved from TechArchives: https://techarchives.irish/how-the-internet-came-to-ireland-1987-97/

Telecommunications Regulations of the People's Republic of China. (2000).

The Guardian. (2002, July 16). *Chinese sites agree to censor content*. Retrieved from The Guardian: https://www.theguardian.com/technology/2002/jul/16/onlinesecurity.internetnews

The National News. (2023, November 11). *Top 12 Cybercrime Trends to Watch for in 2023*. Retrieved from National News: https://thenationalnews.com

Timon, V., Deasy, Z., O'Donnell, S., & Drennan, B. (2023, July 20). *Data Protection Laws and Regulations Ireland 2023-2024*. Retrieved from ICLG.Com: https://iclg.com/practice-areas/data-protection-laws-and-regulations/ireland#:~:text=The%20ePrivacy%20Regulations%20apply%20to,marketing%20from%20outside%20the%20EU.

TransAsiaLawyers. (2016, June 18). *Measures on Internet Information Services*. Retrieved from TransAsiaLawyers: https://www.transasialawyers.com/translation/legis_16_e.pdf

Tsai, K. (2011). How to create international law: the case of Internet freedom in China. *Duke Journal of Comparative & International Law*, 401-403.

Umoru, A. D. (2017, May 5). *What is lost to cybercrime in Nigeria*? Retrieved from The Vanguard: http://www.vanguardngr.com/2017/05/450m-lost-cyber-crime-nigeria-senate/

United Nations. (2011). La Rue F Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression Human Rights Council.

United Nations. (2023, December 1). *Sustainable Development Goals*. Retrieved from SDP Development: https://sustainabledevelopment.un.org/topics/sustainabledevelopmentgoals

Verizon. (2022, January 18). *What is an Internet service provider (ISP)*? Retrieved from Verizon: https://www.verizon.com/about/blog/isp-meaning

Weiss, P. (2023, August 11). *The year ahead: key cybersecurity and privacy issues*. Retrieved from PaulWeiss: www.paulweiss.com

William, D., Dopatka, A., Hills, M., Law, G., & Nash, V. (2010). *Freedom of connection - freedom of expression: the changing legal and regulatory ecology shaping the internet*. Retrieved from Milthailand: http://www.milthailand.org/phocadownload/2011_Files/10_Oct/media/freedompercent20ofpercent20connectionpercent20freedompercent20ofpercent20expression.pdf

Wu, T. (2003). Network neutrality, broadband discrimination. *Journal of Telecommunications and High Technology Law*, 141-176.

Wu, T. (2006). The World Trade Law of censorship and internet filtering. *Chicago Journal of International Law*, 263-287.

Yoo, C. S. (2005). Beyond network neutrality. *Harvard Journal of Law & Technology, 19*(1), 1-77.

Yoo, C. S. (2006). Network neutrality and the economics of congestion. *Georgetown Law Journal*, 1847-1908.

Zarei, B., Asgarnezhad, N., & Noroozi, N. (2019). The effect of Internet service quality on consumer's purchase behaviour: the role of satisfaction, attitude, and purchase intention. *Journal of Internet Commerce*, 197-220.

Zingales, N. (2019). *Oxford Handbook on Intermediary Liability.* NY: Oxford Press.