DECODING DIGITAL COLONIALISM AND SURVEILLANCE CAPITALISM IN THE ERA OF THE GLOBAL DIGITAL DIVIDE: A GLOBAL SOUTH PERSPECTIVE

Dissertation submitted to National Law University and Judicial Academy, Assam

in partial fulfilment for award of the degree of

MASTER OF LAWS/

ONE YEAR LL.M. DEGREE PROGRAMME

Submitted by

Shashank Mall

SM0222027

I Year & II Semester

Supervised by

Dr. Himangshu Ranjan Nath

Assistant Professor of Law

National Law University and Judicial Academy, Assam

June 2023

CERTIFICATE

This is to certify that SHASHANK MALL has completed his dissertation titled "**DECODING DIGITAL COLONIALISM AND SURVEILLANCE CAPITALISM IN THE ERA OF THE GLOBAL DIGITAL DIVIDE: A GLOBAL SOUTH PERSPECTIVE**" under my supervision for the award of the degree of MASTER OF LAWS/ ONE YEAR LL.M. DEGREE PROGRAMME of National Law University and Judicial Academy, Assam.

Date: June, 2023.

Dr. HIMANGSHU RANJAN NATH
Assistant Professor of Law.
National Law University and Judicial Academy, Assam.

DECLARATION

I, SHASHANK MALL, do hereby declare that the dissertation titled **"DECODING DIGITAL COLONIALISM AND SURVEILLANCE CAPITALISM IN THE ERA OF THE GLOBAL DIGITAL DIVIDE: A GLOBAL SOUTH PERSPECTIVE"** submitted by me for the award of the degree of MASTER OF LAWS/ ONE YEAR LL.M. DEGREE PROGRAMME of National Law University and Judicial Academy, Assam is a bonafide work and has not been submitted, either in part or full anywhere else for any purpose, academic or otherwise.

Date: June, 2023.

SHASHANK MALL
SM0222027
National Law University and Judicial Academy, Assam

CONTENTS

Content **Page No.**

ACKNOWLEDGMENT

First and foremost, I wish to extend my profound gratitude to my teacher, guide and mentor, Dr. Himangshu Ranjan Nath, Assistant Professor of Law, National Law University and Judicial Academy, Assam, for his constant guidance, support and supervision in the process of completing my dissertation. I am highly indebted to him for steering my efforts in the right direction with his insightful knowledge and wealth of experience that have constantly helped me throughout my research.

While researching and preparing for this paper, a great deal of my time was spent in accessing the resources available in the library of the university. Therefore, I extend my heartfelt gratitude to the library staff of National Law University and Judicial Academy, Assam. I am also indebted to all the authors of various books, articles and research papers that I consulted and referred to in preparation of this paper.

And lastly, I would like to express my adoration for my parents for giving me the constant encouragement, support and motivation to help me sustain my efforts in successfully completing my dissertation.

Date: June 2023. **SHASHANK MALL**

UID: SM0222027

National Law University and Judicial Academy, Assam

TABLE OF CASES

TABLE OF STATUTES

INDIA

2000 - The Information Technology Act

MALAYSIA

1997 - Computer Crimes Act

1997 - The Digital Signature Act

1998 - Data Protection Act

1998 - Communications and Multimedia Act

2010 - Personal Data Protection Act

2013 - The Financial Services Act

2013 - The Islamic Financial Services Act

NIGERIA

2007 - The National Information Technology Development Agency Act

2015 - The Nigeria Cybercrimes (Prohibition, Prevention, etc.) Act

SINGAPORE

2012 - Personal Data Protection Act

2018 - Cybersecurity Act

SOUTH AFRICA

2002 - Electronic Communications and Transactions Act

2002 - Regulation of Interception of Communications and Provision of Communication related Information Act

2013 - Protection of Personal Information Act

TABLE OF ABBREVIATIONS

S.NO	ABBREVIATION	FULL FORM
1.	ACLU	American Civil Liberties Union
2.	ANPD	Autoridade Nacional de Proteção de Dados
3.	ATT	App Tracking Transparency
4.	AWA	All Writs Act
5.	AWS	Amazon Web Services
6.	CBN	Central Bank of Nigeria
7.	CJEU	Court of Justice of the European Union
8.	CIGI	Centre for International Governance Innovation
9.	CIPL	Centre for Information Policy Leadership
10.	CLOUD	Clarifying Lawful Overseas Use of Data
11.	CMA	Communications and Multimedia Act
12.	CNIL	Commission Nationale de l'Informatique et des Libertés
13.	CPLT	Consejo para la Transparencia
14.	DOJ	Department of Justice
15.	DPO	Data Protection Officer
16.	DPTM	Data Protection Trust Mark
17.	EC	European Commission
18.	ECPA	Electronic Communications Privacy Act
19.	ECTA	Electronic Communications and Transactions Act
20.	EDPB	European Data Protection Board
21.	FBI	Federal Bureau of Investigation
22.	FOIA	Freedom of Information Act
23.	FSA	Financial Services Act
24.	FTC	Federal Trade Commission
25.	GDPR	General Data Protection Regulation
26.	ICO	Information Commissioner's Office
27.	IFSA	Islamic Financial Services Act
28.	IMDA	InfoComm Media Development Authority
29.	ISTAS	International Symposium on Technology and Society

30.	ITA	Information Technology Act
31.	ITU	International Telecommunication Union
32.	LDCs	Least Developed Countries
33.	LGPD	Lei Geral de Proteção de Dados Pessoais
34.	LLDCs	Landlocked Developing Countries
35	MNC	Multinational Corporations
36.	NCC	Nigerian Communications Commission
37.	NDPR	Nigeria Data Protection Regulation
38.	NIMC	National Identity Management Commission
39.	NITDA	National Information Technology Development Agency
40.	NSA	National Security Agency
41.	OECD	Organisation for Economic Co-operation and Development
42.	OSCOLA	Oxford Standard for Citation of Legal Authorities
43.	RICA	Regulations of Interception of Communications and Provision of Communication-Related Information Act
44.	SCCs	Standard Contractual Clauses
45.	SEC	Securities and Exchange Commission
46.	SEO	Search Engine Optimization
47.	SGCA	Singapore Court of Appeal
48.	SSMIs	Significant Social Media Intermediaries
49.	STJ	Superior Court of Justice
50.	TDSF	Trusted Data Sharing Framework
51.	TFEU	Treaty on the Functioning of the European Union
52.	UN-DESA	United Nations Department of Economic and Social Affairs
53.	UPI	Unified Payments Interface
54.	VoIP	Voice over IP

CHAPTER 1

INTRODUCTION

"Surveillance capitalism unilaterally claims human experience as free raw material for translation into behavioural data."

-Shoshana Zuboff[1]

1.1. INTRODUCTION

In recent years, the digital divide has become a major issue of concern in the Global South, where many people lack access to basic digital technologies and infrastructure. This divide is not only about access to technology but also about the ways in which digital technologies are being used to exploit and control people.

The world is increasingly becoming digitalized, and with this comes the potential for the spread of new forms of colonialism and capitalism. In particular, digital colonialism and surveillance capitalism are two related phenomena that have been identified as key factors perpetuating the global digital divide.

In this era of the global digital divide, the Global South is at the forefront of the struggle against digital colonialism and surveillance capitalism. Digital colonialism refers to the ways in which the Global North exerts control over the digital sphere of the Global South, while surveillance capitalism is the practise of exploiting personal data for profit. In this paper, we will examine the impact of digital colonialism and surveillance capitalism on the Global South and explore how these practises can be resisted.

The digital divide refers to the unequal distribution of information and communication technologies (ICTs) across the world. According to the International Telecommunication Union, 66% of the world's population had access to the internet

[1]Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile Books England 2019).

in 2022[2]. This leaves almost half of the world's population without access to the benefits of digital technologies such as e-commerce, e-learning, and e-health. The digital divide is not only an issue of access but also of affordability, quality, and relevance. Many people in the Global South have limited access to affordable, reliable, and fast internet services, and even when they do, the content they access is often irrelevant to their local contexts and languages.

Digital colonialism refers to the ways in which the Global North exerts control over the digital sphere of the Global South. This can take many forms, including the dominance of Western internet companies, the imposition of Western values and standards, and the use of digital technologies for surveillance and control. It is not a new phenomenon; it builds upon a long history of colonialism, imperialism, and neo-colonialism that has shaped the relations between the Global North and the Global South.

The dominance of Western internet companies in the Global South is one of the most visible forms of digital colonialism. Companies like Google, Facebook, Amazon, and Microsoft have become ubiquitous in the Global South, providing services that are essential for communication, information, and entertainment. However, these companies often operate under Western standards and values, ignoring the local context and languages of their users. This can lead to the marginalisation of local cultures and the dominance of Western cultural values.

The imposition of Western values and standards is another form of digital colonialism. Western governments and international organisations often impose their standards and values on the Global South, using digital technologies as a means of control. Many countries in the Global South have been pressured to adopt Western-style intellectual property laws, which can limit their access to knowledge and restrict their ability to innovate. Similarly, many they have been pressured to adopt Western-style cybersecurity laws, which can be used to suppress dissent and restrict freedom of speech.

Surveillance capitalism is the practise of exploiting personal data for profit. It has become widespread in the digital sphere as companies collect vast amounts of data

[2]International Telecommunication Union (ITU) statistics, 'Measuring Digital Development: Facts and Figures.' (2022) <https://www.itu.int/itu-d/reports/statistics/2022/11/24/ff22-foreword/> accessed 30 June 2023.

about their users' online behaviour and use it to target them with personalised ads. While this practise is often seen as harmless, it can have serious implications for privacy, democracy, and human rights.

In the Global South, surveillance capitalism can be particularly harmful. Many countries in the Global South have weak data protection laws and limited oversight of the use of personal data. This leaves users vulnerable to exploitation by Western internet companies and governments. Additionally, the use of digital technologies for surveillance can be used to suppress dissent and restrict freedom of speech.

The Global South faces considerable challenges from digital colonialism and surveillance capitalism, which put sovereignty, human rights, and democracy at risk. It is imperative to resist in order to safeguard these values and promote indigenous innovation. The global struggle requires collaboration and solidarity among actors in both the Global North and the Global South. The advancement of the campaign against digital colonialism and surveillance capitalism may be achieved through the development of alternative technologies, the implementation of robust data protection laws, and the promotion of digital literacy and awareness.

1.2. STATEMENT OF PROBLEM

In the modern technology era, a few major countries and corporations have monopolised the digital economy, creating the global digital gap.

Surveillance capitalism, in which companies collect and monetize personal data, has further complicated digital colonialism in poor countries from The Global South—Africa, Asia, and Latin America—and left them economically marginalised. The sale of personal data has become more common in the digital economy. Multinational technology corporations from developed countries have profited from user data collection, often without their consent.

Global South individuals' privacy and liberties have been reduced by digital colonisation. A few large corporations in developed countries have consolidated power by monetizing individual data. These entities have an advantage over companies in emerging countries because they can collect and evaluate massive amounts of data.

Personal data commercialization has exploited people in the Global South, who have become profitable for corporations in the Global North. Building digital economies and competing in the global digital market is difficult for developing countries. The Global South has suffered economically and socially from unequal digital infrastructure, technical access, and personal data exploitation.

These concerns must be addressed to establish a fairer digital world where the Global South can compete with the Global North and expand its digital economy.

1.3. LITERATURE REVIEW

Bottis and Bouchagiar[3] (2018) delves into the process of modifying personal data into identifiable information such as names and browsing histories, which is currently being converted into a marketable asset. The transition has transpired because of the escalating significance of individual data for commercial entities, advertisers, and governmental bodies. The rationales underpinning the commodification process encompass focused advertising, market analysis, and tailored amenities.

The commercialization of individual data presents several challenges. The acquisition and utilisation of individualised information elicit apprehensions regarding the violation of confidentiality, monitoring, and plausible exploitation by external entities. The loss of control over personal information poses ethical implications for individuals, and the growing amount of personal data serves as a magnet for cybercriminals.

Moreover, the acquisition of informed consent is hindered by intricate procedures for gathering and utilising data. One of the challenges pertains to the absence of all-encompassing legal frameworks and regulations that oversee personal data. The article examines the involvement of governments, industry standards, and international agreements in tackling the concerns.

The article primarily addresses the obstacles associated with the commodification of personal data in the realm of big data. However, it fails to consider other significant factors, including social, legal, and economic ramifications, as well as the viewpoints of various stakeholders.

[3]Maria Bottis and George Bouchagiar, 'Personal Data v. Big Data: Challenges of Commodification of Personal Data' (2018) 8 Open Journal of Philosophy <https://doi.org/10.4236/ojpp.2018.83015> Accessed 30 June 2023.

Furthermore, the absence of empirical research or case studies constrains its capacity to offer pragmatic insights. Moreover, it is worth noting that the article's publication date is 2018, which implies that it may not encompass the most recent advancements in the domain, such as nascent technologies, dynamic regulatory structures, and shifting public perspectives regarding data confidentiality.

Zuboff[4] (2019) in her literary work delves into the emergence and ramifications of surveillance capitalism on the populace, communal structure, and the financial system. The author conducts an analysis of the historical context of surveillance capitalism and underscores its divergence from conventional capitalism as it seeks to forecast and manipulate human behaviour for financial gain.

She expounds upon the techniques employed in the acquisition and utilisation of personal data, underscoring its multifaceted application in not only targeted advertising but also the manipulation and influence of human behaviour.

The notion of "instrumentarian power" is put forward, denoting the unparalleled authority that surveillance capitalists wield over both individuals and societies. The consolidation of power gives rise to apprehensions regarding the potential for manipulation and coercion, which can undermine the autonomy of individuals and their freedom to make choices.

The analysis extends to the wider societal ramifications, encompassing issues such as the erosion of democratic principles and individual liberties, the amplification of social disparities, and the intensification of power differentials.

The concluding segments underscore the significance of resistance and collective action as effective measures to counter the impact of surveillance capitalism. The individual in question espouses the importance of reclaiming privacy rights at the individual level, creating novel legal frameworks, and cultivating heightened public consciousness on the matter.

The author's scholarly contributions have initiated significant dialogues pertaining to the domains of privacy, data ethics, and power structures.

[4]Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power (*London, England, Profile Books, London, England 2019).

Nevertheless, criticisms and limitations have been acknowledged. The broad and overarching statements fail to acknowledge the intricacies and diversities inherent in the subject matter, thereby neglecting to acknowledge situations where the collection of data can prove advantageous.

The predominant negative depiction of surveillance capitalism fails to acknowledge the potential positive facets of this phenomenon. The absence of a thorough empirical investigation and a comprehensive strategy that involves industry stakeholders and integrates diverse perspectives is a notable limitation of the book.

Furthermore, the analysis exhibits a tendency to ascribe an undue amount of power to technology while disregarding the impact of human agency and decision-making that is influenced by economic and political factors.

Couldry and Mejias[5] (2019) were the first to introduce the term 'Data Colonialism' through this paper. According to them, the emergence of Big Data has led to the development of a novel type of colonialism referred to as data colonialism.

According to their assertion, corporations and governments engage in the exploitation of personal data belonging to individuals and communities, thereby transforming it into a commodity that serves their own interests. The phenomenon of exploitation is manifested through various mechanisms, including extraction, appropriation, analysis, and prediction.

According to the authors, data colonialism constitutes a peril to personal agency, confidentiality, and self-respect and further erodes the foundations of democratic governance. The argument posits that the extensive and intrusive surveillance facilitated by Big Data has the capacity to manipulate public sentiment and stifle opposition.

Nevertheless, the article exhibits certain constraints. The primary focus of this study is on data colonialism as it pertains to Western contexts, with a relative lack of attention given to its manifestations in other regions and socio-political contexts.

[5]Nick Couldry and Ulises A. Mejias, 'Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject' (2019) 20(4) Television & New Media, 336–349. <https://doi.org/10.1177/1527476418796632> accessed 30 June 2023.

The presentation of Big Data in the text appears to be somewhat biased, as it primarily highlights the adverse effects associated with it. Subsequent investigations may offer a more equitable evaluation by delving into the plausible affirmative ramifications of Big Data, encompassing scientific progress, communal well-being, and societal growth.

Furthermore, the scholarly article could provide a more comprehensive analysis of the tactics utilised by individuals and communities to resist and exert agency against the phenomenon of data colonialism, thereby contributing to a more nuanced comprehension of the topic. The text provides a concise mention of the necessity for policy interventions; however, it falls short of thoroughly examining plausible regulatory frameworks.

Subsequent investigations may delve into the legal and governance aspects, taking into account both domestic and global strategies aimed at safeguarding personal liberties and tackling the power asymmetries that are inherent in the phenomenon of data colonialism.

Kwet[6] (2019) provides a critical examination of the relationship between digital technologies, US imperialism, and the Global South. Kwet states that the proliferation of digital technologies by American tech corporations and the sway of the United States over worldwide digital governance frameworks have given rise to a variant of digital colonialism. This phenomenon serves to strengthen pre-existing power differentials and sustain neo-colonial practises.

Kwet highlights that the Global South is subjected to the hegemony of Western corporations, particularly those originating from the United States, through the dissemination of digital technologies, thereby resulting in a rise in socio-economic disparity.

Kwet brings attention to the reliance of the Global South on digital technologies and platforms originating from the West, leading to a potential relinquishment of authority over data, resources, and decision-making. This phenomenon serves to perpetuate the neo-colonial dynamic between the Global North and South, as it allows for the

[6]Michael Kwet, 'Digital colonialism: US empire and the New Imperialism in the Global South.' (2019) 60(4) Race & Class. DOI: 10.1177/0306396818823172 <https://ssrn.com/abstract=3232297> accessed 30 June 2023.

extraction of value from data produced in the Global South by Western corporations, while simultaneously constraining local autonomy and economic advancement.

The author elucidates the role of digital technologies in enabling surveillance and control by both state and non-state actors. They further highlight that certain US-based technology companies have been accused of aiding authoritarian regimes in their efforts to monitor and quell dissent.

Kwet offers a critique of the prevailing global digital governance frameworks, namely the ITU and ICANN, which are predominantly influenced by the US, and argues that they function as tools of US imperialism.

Although Kwet's theoretical analyses and anecdotal evidence are convincing, the article would benefit from more robust empirical validation, such as case studies and quantitative data.

Furthermore, a comprehensive examination could take into account the functions of other dominant nations, such as Russia, the United Kingdom, or the European Union, in the phenomenon of digital colonialism. Recognising the multiplicity and variability present within the Global South would enhance the analytical process.

Coleman[7] (2019) explores the concept of digital colonialism, and focuses specifically on Africa, where there is a growing concern regarding the scramble for user data and the associated implications for economic, political, and social power structures.

The research highlights the exploitation of African users through data extraction, drawing parallels to the historical practise of colonialism. Foreign entities, such as technology conglomerates and data intermediaries, amass extensive quantities of data from African users for the purposes of targeted advertising, algorithmic profiling, and political manipulation.

The phenomenon sustains the unequal distribution of power between the Global North and Africa, thereby compromising the prospective advantages of digital technologies for the latter. It emphasises the constraints of data protection legislation in Africa, which are further exacerbated by insufficient knowledge and proficiency in digital technology among users, thereby exposing them to potential exploitation. It advocates

[7]Danielle Coleman, 'Digital Colonialism: The 21st Century Scramble for Africa through the Extraction and Control of User Data and the Limitations of Data Protection Laws' (2019) 24 Mich J Race & L 417.

for heightened consciousness and more robust legal structures and endeavours to narrow the gap in access to technology.

Nevertheless, the research exhibits certain deficiencies like the absence of attention to regional nuances and inter-country distinctions within Africa presents a potential limitation in comprehending the complexities of the obstacles encountered.

The examination of the roles and responsibilities of diverse stakeholders, such as governments, corporations, civil society organisations, and users, is limited. A more comprehensive comprehension of digital colonialism could be achieved through comparative analysis that extends beyond the African continent and delves into historical parallels.

Furthermore, the exploration of potential solutions and mitigation strategies is limited. Further studies may explore alternative regulatory methodologies, cross-border partnerships, community-based initiatives, and safeguarding the rights and interests of African users.

Sahbaz[8] (2019) discusses the potential risks of Artificial Intelligence (AI) in perpetuating new forms of colonialism. The author argues that the technological advancements in AI could create a power imbalance between developed and developing countries, leading to new forms of exploitation and domination.

Sahbaz delves into the prospective dangers of artificial intelligence in perpetuating new characteristics of colonialism. The article underscores the historical correlation between colonialism and the exploitation, oppression, and underdevelopment of developing countries.

The author's argument is that the implementation of artificial intelligence (AI) has the potential to amplify already-existing power differentials. This is because AI frequently relies on data procured from developing nations without proper authorization and may also lead to the automation of jobs, thereby affecting the economic landscape of these regions.

[8]Ussal Sahbaz, 'Artificial Intelligence and the Risk of New Colonialism' (2019) Horizons: Journal of International Relations and Sustainable Development, No. 14, The Importance of being earnest: Geopolitics of Realism (Summer 2019), pp. 58-71, Center for International Relations and Sustainable Development.

The article expresses apprehension regarding the utilisation of AI in surveillance and control, which could potentially result in violations of human rights and the perpetuation of global power dynamics.

However, the article exhibits certain constraints. The provided discussion exhibits a deficiency in presenting a comprehensive explanation of artificial intelligence (AI) and falls short in clarifying technologies and applications that are relevant to the argument at present.

The discourse primarily centres on the possible risks associated with artificial intelligence while neglecting to address the prospective advantages that AI could offer to emerging economies, such as the promotion of financial expansion.

Furthermore, the research fails to incorporate the current literature on artificial intelligence and its impact on development, thereby overlooking prospects for a more sophisticated comprehension and examination of initiatives and structures aimed at tackling these issues.

Finally, although advocating for heightened consciousness and moral standards, the article falls short of providing specific directives for policymakers tasked with minimising potential hazards.

Greenwood[9] (2020) as part of the book 'Mapping Crisis: Participation, Datafication and Humanitarianism in the Age of Digital Mapping,' wrote a chapter on 'Data colonialism, surveillance capitalism and drones' which is an insightful exploration of the intersection of digital mapping, data colonialism, and surveillance capitalism in the age of humanitarianism.

The chapter by Greenwood provides a critical analysis of the intersection between data colonialism, surveillance capitalism, and humanitarianism. The author's focus is on the use of drones for disaster response.

The author states that the historical ramifications of colonialism have engendered a scenario where data ownership is concentrated among dominant entities, thereby giving rise to the phenomenon of 'data colonialism.'

[9] Faine Greenwood, **'**Data colonialism, surveillance capitalism and drones.' in *Mapping Crisis: Participation, Datafication and Humanitarianism in the Age of Digital Mapping Book* (University of London Press, Institute of Commonwealth Studies, 2020).

The phenomenon of surveillance capitalism refers to the concentration of data ownership, which enables private companies to monetize individuals' data without their explicit consent.

Greenwood's analysis focuses on the application of drone mapping technology in disaster-stricken areas, shedding light on the workings of surveillance capitalism within the realm of humanitarian aid. The data acquired through the use of unmanned aerial vehicles is frequently not leveraged for the betterment of the general populace but rather serves to enhance the financial gain of the private entities responsible for its collection.

The author promotes the notion of decentralised ownership of drone data, underscoring its classification as a public good, and proposes that the objective can be accomplished by utilising open-source software and establishing data-sharing agreements.

Greenwood's analysis highlights significant ethical considerations pertaining to data ownership and surveillance capitalism. However, it is important to note that the chapter has certain limitations.

The current research on drone mapping in disaster zones falls short of providing a thorough examination of the viewpoints and encounters of the affected communities. Consequently, there is a need for additional investigation to comprehend their reactions towards this technological intervention.

Furthermore, the exclusive emphasis on unmanned aerial vehicles disregards alternative technologies such as satellites and terrestrial sensors, which are also utilised in disaster management and rehabilitation endeavours.

A comprehensive understanding of the ethical implications of data ownership and surveillance capitalism within humanitarianism can be achieved through a more extensive analysis of diverse technologies.

Viljoen[10] (2021) explores the principles and practices that should govern the use of data in the digital age. According to Viljoen, conventional data governance models that revolve around safeguarding individual privacy and data protection are inadequate for tackling the intricacies of contemporary data systems.

[10]Salome Viljoen, 'A Relational Theory of Data Governance' (2021) 131 Yale L J 573.

The author proposes an alternative perspective on data governance, which centres on a relational framework that underscores the social, economic, and political connections that are inherent in data practises.

The article provides a historical account of data governance and highlights two prevailing paradigms: the market-oriented model, which views data as a tradable commodity, and the regulatory model, which relies on legal frameworks.

According to Viljoen, the models exhibit a deficiency in addressing wider social and political ramifications. The theoretical framework proposed by the author centres around the concepts of reflexivity, reciprocity, and responsibility. This framework places significant emphasis on the cultivation of self-awareness, the equitable consideration of stakeholder interests, and the establishment of accountability.

The author employs instances from the domains of healthcare, finance, and government to demonstrate the applicability of the theory in question. The author emphasises the potential of this theory to tackle issues such as the concentration of power, the erosion of privacy, and algorithmic bias.

The paper makes a noteworthy contribution to the literature on data governance by underscoring the importance of social and political relationships in data practises.

Nonetheless, the analysis presented falls short in terms of delving into the practical hurdles that may arise during implementation as well as the potential ramifications of nascent technologies such as artificial intelligence and machine learning.

Moreover, the article predominantly centres on Western liberal democracies, thereby overlooking worldwide viewpoints.

Future research may fill these gaps by scrutinising impediments to operationalizing the relational theory, scrutinising the impact of technology on data practises, and delving into the theory’s relevance in heterogeneous cultural and political milieus, encompassing worldwide concerns such as data sovereignty and surveillance.

Kakar[11] (2021) discusses several issues related to digitalization and its impact on society, specifically focusing on algorithmic bias, digital colonialism, and the decentralization of the internet.

Kakar's article explores the phenomenon of algorithmic bias within American healthcare institutions and its effects on historically marginalised populations. It highlights the importance of conducting comprehensive research to reveal occurrences of institutional partiality that may have negative effects on these particular groups.

The research findings indicate that a commonly employed algorithm in American healthcare facilities exhibited discriminatory tendencies towards African American patients, thereby implying the existence of institutional prejudice that engenders a sense of mistrust and bias within the healthcare sector.

The presence of bias in algorithms creates obstacles for marginalised communities in accessing healthcare, underscoring the significance of ethical considerations in the development of such algorithms.

The article additionally highlights the wider ramifications of digitalization on underprivileged communities and emphasises the necessity of ethical artificial intelligence principles that prioritise the welfare of the majority. Algorithmic decision-making has the potential to detect patterns of systemic exclusion.

However, it has also been observed that this approach has led to the marginalisation and disempowerment of minority groups, particularly in the context of predictive policing. The prioritisation of ethical considerations is crucial in the development of artificial intelligence to avoid the amplification of pre-existing systemic inequalities.

Moreover, the article examines the concept of digital colonialism and its impact on underprivileged communities, particularly in developing regions of the world. The text advocates for alterations to digital devices to prevent the circumvention of nearby villages. It highlights the efficacy of initiatives such as the 'FreedomBox' in furnishing decentralised technology and authority to local communities.

[11]Gyanda Kakar, 'Cognitive Dysphoria: Evaluating the Paradigm Shift of Artificial Intelligence Technology in Digital Colonialism' (2021) 2 Indian J Artificial Intel & L 7.

The article highlights occurrences of digital colonisation, such as the billing policies of Google Play, and emphasises the necessity of developing domestic alternatives and legislative measures to safeguard digital rights and counteract digital colonialism.

However, the article acknowledges the lack of all-encompassing research on the ramifications of algorithmic decision-making and digital colonialism on underprivileged communities. Further investigation, the availability of exclusive algorithms, and private health data are required.

Furthermore, it acknowledges the constrained availability of medical care due to institutional prejudice and a lack of confidence in the healthcare infrastructure, which intensifies health inequalities.

Paco[12] (2022) covers the topic of data colonialism, its impact on personal privacy, and the measures that can be taken to protect it. The article discusses the concept of data colonialism, which pertains to the appropriation of economic and political influence from individuals and countries through the unconsented exploitation of personal data by major technology corporations.

The paper underscores the ethical implications and privacy breaches linked to this practise, along with its capacity to disseminate false information and disrupt socio-political environments.

The author proposes that data localization mandates, which necessitate the storage and processing of data within a nation's territorial boundaries, have been instituted as a form of retaliatory action. Nonetheless, they advise against the plausible exploitation of individual data by governmental entities under such legislation.

Other suggested alternatives involve advocating for domestic innovation that is not reliant on foreign technology corporations and regarding data as a national asset, with corporations compensating for its utilisation in the development of domestic infrastructure.

The paper recognises the necessity of achieving equilibrium between the protection of personal privacy rights and the promotion of economic interests, particularly in light of India’s expanding digital economy.

[12]Sarah A. Paco, ‘Data Colonialism, the Danger It Poses to India's Democracy, and the Effectiveness of Data Localization Laws as Resistance’ (2022) 48 Rutgers Computer & Tech LJ 254.

The statement underscores the significance of regulating the operations of American Big Tech corporations while avoiding any authoritarian tendencies in order to promote domestic innovation while simultaneously protecting personal data.

Nevertheless, the article exhibits certain constraints. The analysis fails to take into account the broader social and cultural ramifications of data colonialism, instead placing disproportionate emphasis on its economic and political outcomes. Insufficient attention is given to the potential negative consequences and constraints of suggested policy remedies.

Furthermore, the article exhibits a lack of a precise explanation of the term 'data colonialism' and fails to distinguish it from associated notions. The absence of clarity in the presentation of information may hinder comprehension of the extent and consequences of the issue.

Heeks[13] (2022) discusses the concept of 'adverse digital incorporation' and its implications for digital inequality in the global South. The article discusses the concept of adverse digital incorporation, denoting the disparate consequences and value appropriation encountered by socioeconomically disadvantaged individuals and collectives upon their integration into digital frameworks.

The argument posits that a more comprehensive comprehension of digital inequality should encompass power dynamics, access to design processes and resources, as well as social structures. The author recognises the capacity of marginalised communities to navigate unfavourable digital integration through decision-making, opposition, and bargaining.

However, the article exhibits shortcomings in providing a thorough examination of the interplay between intersectionality and technological determinism in influencing the development of digital inequality.

The study offers a restricted set of policy implications and recommendations to tackle the issue of negative digital integration. It highlights the necessity for additional research in this domain. The primary emphasis is on the issue of digital inequality in

[13]Richard Heeks, 'Digital inequality beyond the digital divide: conceptualizing adverse digital incorporation in the global South', (2022) 28(4) Information Technology for Development pp. 688-704. DOI: 10.1080/02681102.2022.2068492.

the Global South, with a limited examination of the specific dynamics at the regional or national level.

Following studies, initiatives should undertake meticulous examination of individual cases, delve into the ramifications of technology design decisions, formulate practical policy suggestions, and take intersectionality into account as a means of augmenting our comprehension of and resolving digital disparity more efficiently.

Jimenez and Oleson[14] (2022) offers a comprehensive examination of the concept of data crimes in the context of digital capitalism. This research investigates the phenomenon of data crimes in the context of digital capitalism, with a particular emphasis on the exploitation of user data and the infringement of competition rules and regulations.

It highlights the correlation between the ascent of neoliberalism and the pervasiveness of corporate offences, emphasising the importance of both theoretical and pragmatic remedies to tackle corporate wrongdoing.

The Facebook case study serves as a significant example of the severity of data-related offences, which include breaches of privacy and anti-competitive conduct. The article introduces the notion of 'data colonialism', which pertains to the act of appropriating human life for the purpose of extracting data and generating profit.

The article advocates for the dismantling of the colonial framework of indifference within which digital corporations operate. The need for a more comprehensive examination of international jurisdiction and the difficulties associated with ensuring the accountability of multinational corporations are recognised considering the global nature of data crimes.

The acknowledgement of the power asymmetry existing between corporations and individuals is prevalent, albeit not exhaustively investigated. Therefore, a more profound analysis of the fundamental power dynamics in the context of digital capitalism is warranted.

The article exhibits a substantial reliance on theoretical arguments while falling short of providing a comprehensive empirical evidence base. This highlights the necessity

[14]Aitor Jimenez & J. C. Oleson, 'The Crimes of Digital Capitalism' (2022) 48 Mitchell Hamline L Rev 971.

for additional research and data analysis. It acknowledges the difficulties posed by the existing legal framework but refrains from delving deeply into regulatory strategies or presenting specific remedies. The practical implications of the article could be improved by conducting a thorough examination of regulatory frameworks and potential reforms.

Thatcher and Dalton[15] (2022) delve into the intricate relationship between geographical and technological systems and their impact on our lives. The paper discusses the constraints of data-driven systems, specifically in tackling intricate concerns such as regulating airborne viruses.

The opacity of algorithms has been a source of concern for some individuals, as it has altered our interaction with technology from a dialogue-based approach to one where technology assumes a speaking role on our behalf. The proprietary nature of algorithms, which maintain their inner workings as trade secrets, contributes to this issue.

The paper delves into the pervasive influence of quantification and data production in our daily lives, which has resulted in a perceived reliance on algorithms to shape our behaviours and results.

The authors recognise the efficacy of algorithms in enhancing digital presentations and shaping results, while also acknowledging the inherent ambiguity of specificity and subjective encounters. The focal point of their argument centres on the inherent conflict between the potency of algorithms and the individual's yearning for autonomy in managing their personal data.

Furthermore, the authors emphasise the disparate effects of data and algorithms on diverse demographics, thereby reinforcing pre-existing disparities and impeding equitable access to resources and prospects.

The article advocates the promotion of active resistance and solidarity to mitigate the possible negative consequences of data-driven systems. The statement underscores the significance of questioning and scrutinising these systems and advocates for individuals to participate actively in the decision-making procedures. The proposition

[15]Jim E. Thatcher and Craig M. Dalton, 'What are our data, and what are they worth?' (2022) Data Power: Radical Geographies of Control and Resistance, pp.46–64. Pluto Press. <https://doi.org/10.2307/j.ctv249sg9w.9.> accessed 30 June 2023.

put forth by the authors posits that authentic forms of resistance and solidarity have the potential to engender outcomes that are characterised by greater levels of equity.

However, a wider range of focused examples to support the article's arguments would have strengthened its analysis. The material briefly alludes to ethical considerations; however, it does not extensively explore them or present a comprehensive analysis of the potential advantages of data-driven technologies.

Moreover, the examination of alternative methodologies or remedies is not thoroughly investigated. The content could be enhanced by incorporating additional concrete illustrations, a more comprehensive analysis of ethical ramifications, an equitable viewpoint, and an examination of substitute resolutions.

Sulkowski and Others[16] (2022) discuss the regulation of data collection and usage, exploring various considerations and potential solutions. In contrast to only focusing on prohibitions, the paper argues for the necessity of proactive rules that address data collection and use. To get better results, it advises combining current data collection techniques with a comprehensive comprehension of how companies affect systems.

The authors raise doubts about the effectiveness of unconscionability and contracts of adhesion in protecting privacy rights in the context of developing technology. They also take into account the need for private blockchains with public agency access for data monitoring in order to ensure data integrity and combat fraud.

The study looks at more general challenges, including data deletion and deciding what data should never be kept. It suggests exempting small to medium sized organisations from the requirement to monitor and utilise data, raising the question of whether there should be a size barrier. The possible hazards connected to growing data collection, such as the purposeful or inadvertent exposure of private data, are discussed, highlighting the necessity of constant risk assessment by professionals.

It also criticises the efficacy of straightforward year-end reporting and advocates implementing additional measures to evaluate how corporations affect people and the environment. To reduce emissions, it explores the merits of mandating the purchase of carbon credits. The idea of automated offsets is offered, which may cause controversy

[16]Adam J. Sulkowski, Danielle Blanch-Hartigan, Caren Beth Goldberg, Amy K. Verbos, Mao liang Bu and Remy Michael Balarezo Nunez, 'Systems Theory, Surveillance Capitalism, and Law: Native Wisdom and Feedback Loops to Boost the Constructive Use of Big Data' (2022) 20 Colo Tech LJ 121.

not just in environmental situations but also in social contexts like affirmative action and diversity initiatives.

The authors urge policies that go beyond bans and offer advice on the best ways to collect and use data. They contend that adopting these practises satisfies fiduciary obligations, lowers the possibility of negligence claims, and ultimately produces superior results.

The study discusses many issues linked to data collection, consumption, and privacy protection, stressing the dangers and problems related to greater data accumulation, even if it does not directly describe surveillance capitalism.

Beydoun[17] (2022) explores the topic of digital surveillance and its implications for marginalized communities, with a particular focus on the surveillance practices of the Chinese government in Xinjiang and the Egyptian government's use of surveillance to suppress the Muslim Brotherhood.

It discusses the increasing use of surveillance technologies and the need to examine their impact on society. The paper refers to the implementation of sophisticated surveillance technologies in Xinjiang by the Chinese authorities, with a focus on the Uyghur Muslim community.

The paper elucidates the impact of the incorporation of digital surveillance technologies, which has led to the proliferation of mass surveillance, detention, and egregious violations of human rights.

Likewise, the use of digital surveillance by the Egyptian government, frequently employing Chinese technology, has resulted in the curtailment of political expression and religious stigmatisation, particularly targeting the Muslim Brotherhood and its affiliates.

The idea of the 'society of subjugation' is presented, indicating that the aims of surveillance surpass mere regulation and encompass the oppression of specific groups.

[17]Khaled Ali Beydoun, 'The New State of Surveillance: Societies of Subjugation' (2022) 79 Washington & Lee Law Rev 769.

The author conducts an investigation into the effects of digital surveillance on Muslim communities in Egypt, with a particular emphasis on the selective targeting of individuals on the basis of their religious practises.

The inquiry speculates as to whether the United States has the potential to transform into a society of subjugation, wherein communities of colour that are excessively policed are regarded as areas of surveillance where violence, discipline, and control converge. The discourse surrounding surveillance technologies, such as Big Data Policing, centres on their capacity to augment police authority and jeopardise underprivileged populations.

The paper advocates for a reassessment of prevailing surveillance theories, emphasising the need for a more comprehensive perspective that takes into account the demographic characteristics of surveillance subjects and the socio-political milieu in which surveillance is conducted. It highlights the psychological impact of perpetual monitoring and underscores the imperative to safeguard liberties and alleviate damage in underprivileged populations.

The author's primary focus is on the effects of digital surveillance on marginalised communities and advocates for a more comprehensive comprehension of surveillance that extends beyond mere control.

1.4. AIMS OF THE STUDY

The aim of this research is to examine the concepts of digital colonialism and surveillance capitalism in relation to the global digital disparity, with a particular emphasis on the perspective of the Global South.

This research aims to evaluate the effects of digital colonialism and surveillance capitalism on the Global South, a region that comprises countries primarily situated in Africa, Asia, and Latin America.

The persistence of the digital divide in the Global South, despite the rapid expansion of digital technologies and the internet, is a topic that is pertinent to this study. Specifically, the study aims to investigate the role of digital colonialism and surveillance capitalism in perpetuating this divide.

The aim of the research is to examine issues pertaining to privacy and individual autonomy that arise because of the collection and utilisation of private data. Moreover, the uneven allocation of power in digital colonialism has the potential to worsen societal disparities and introduce new forms of exploitation.

The research aims to investigate alternative modes of digital governance as perceived through the lens of the Global South. The research will delve deeper into alternative digital governance models that place emphasis on the requirements and issues of individuals residing in the Global South.

1.5. OBJECTIVES OF THE STUDY

To attain a precise depiction of the present context, it is imperative to conduct research on the following objectives:

(i) To conduct a critical analysis of the concepts of digital colonialism and surveillance capitalism.

(ii) To analyse the historical and structural elements that have played a role in the emergence of the digital divide between the Global North and South.

(iii) To examine the strategies used by multinational corporations to leverage their influence and gather information from users in the Global South.

(iv) To examine the extent to which governments in the Global South are involved in enabling or impeding digital colonialism and surveillance capitalism.

(v) To scrutinise the legal and regulatory frameworks of the Global South that facilitate digital colonialism and surveillance capitalism.

1.6. RESEARCH QUESTIONS

The research questions presented below will be used to investigate the topic of this paper in accordance with its stated objectives.

(i) What are the fundamental characteristics and features of digital colonialism and surveillance capitalism?

(ii) What are the historical and structural factors that have given rise to the inequality in the development of digital technologies and infrastructure between the Global North and South?

(iii) What are the strategies used by multinational corporations and technology firms to acquire data from users in the developing countries of the Global South?

(iv) What are the governmental policies and regulations that have been formulated in the Global South to safeguard the rights and interests of users in the digital domain?

(v) How do legal frameworks and data regulations impact the privacy and autonomy of users in the Global South?

1.7. SCOPE AND LIMITATIONS OF THE STUDY

This paper focuses on how to deal with the above-mentioned aspects to find out whether currently available treaties, conventions, protocols or arrangements are adequate in dealing with the type of situation that Global South states are currently facing regarding digital privacy and protection.

The scope of the study is to explore the concepts of digital colonialism and surveillance capitalism in the context of the global digital divide from a Global South perspective. The aim is to examine the impact of these phenomena on the Global South, identify the ways in which they perpetuate the digital divide, and explore the ethical and political implications of their existence. Additionally, the aim is to explore potential strategies for challenging digital colonialism and surveillance capitalism and developing more equitable forms of digital governance.

This research is subject to various limitations. Firstly, the analysis is based on secondary sources instead of empirical evidence, thereby posing challenges in arriving at conclusive findings.

Secondly, the unavailability of information regarding the collection of personal data by corporations may limit understanding of the practical consequences, particularly among individuals residing in the Global South.

Lastly, the research is grounded in established legal and theoretical frameworks, which may limit the scope of the investigation to concepts rather than encompassing the wider practical implications of digital colonialism and surveillance capitalism in the Global South.

1.8. RESEARCH METHODOLOGY

The legal research approach used is limited to doctrinal legal research, historical, analytical and descriptive methodology, including case studies and narratives.

Primary and secondary sources of data have been used. Primary sources such as the international conventions, protocols, official documents and reports have been referred to. Secondary sources such as books, law journals, articles, encyclopaedia and online database have also been relied upon.

The citation style being adhered to is The Oxford University Standard for Citation of Legal Authorities (OSCOLA) 4th edition and OSCOLA 2006 for citing international law section.

1.9. RESEARCH DESIGN

The **First Chapter** entitled 'INTRODUCTION' begins with a concise introduction to the subject matter under consideration, a specified aim and objective of the research, the study's scope and restrictions, a literature review, research problem, a research methodology, and a research design.

The **Second Chapter** entitled 'CONCEPTUALISATION OF DIGITAL COLONIALISM AND SURVEILLANCE CAPITALISM' examines the concepts of digital colonialism and surveillance capitalism in detail. It investigates the different ways in which these concepts manifest themselves in the digital realm, including how digital technologies are used to maintain colonial power relations and how the collection and analysis of personal data is used for profit-making. It addresses the global digital divide through an examination of the historical and structural causes that have contributed to the disparity in the development of digital technologies and infrastructure between the Global North and the Global South.

The **Third Chapter** entitled 'ROLE OF MULTINATIONAL CORPORATIONS IN DIGITAL COLONIALISM AND SURVEILLANCE CAPITALISM' explores the ways in which multinational corporations have leveraged their power to exploit and extract data information from users in the Global South. This includes analysing the business models of these companies and the ways in which they have used their economic and political power to dominate the digital realm in the Global South.

The **Fourth Chapter** entitled 'ROLE OF GLOBAL SOUTH GOVERNMENTS AND POLICYMAKERS IN DIGITAL COLONIALISM AND SURVEILLANCE

CAPITALISM' investigates the role of governments and policymakers in the Global South in facilitating or resisting digital colonialism and surveillance capitalism. This involves analysing the policies and regulations that have been put in place to govern digital technologies and the internet in the Global South, and how these policies have either contributed to or challenged the digital divide.

The **Fifth Chapter** entitled 'CONCLUSION, FINDINGS AND SUGGESTIONS' encompasses conclusions found because of this extensive study and aims to examine the technological practices that enable digital colonialism and surveillance capitalism, including the role of algorithms, data collection, and data analysis. The study put forth findings that explain how these digital technologies are used to perpetuate power imbalances and how they can be reconfigured to challenge dominant power structures.

CHAPTER 2

CONCEPTUALISATION OF DIGITAL COLONIALISM AND SURVEILLANCE CAPITALISM

The idea of monitoring has taken on an altogether new meaning in the modern era of accelerated advances in technology and globalisation. A complex web of covert and overt surveillance systems has emerged as a result of the development of technological advancements and their pervasive integration into our everyday lives. This has significant ramifications for both people and society at large.

This chapter analyses the concepts of both digital capitalism and surveillance capitalism, highlighting the differences between them and examining the intricate interactions connecting these two interwoven phenomena. However, first, we need to understand the current global digital divide between the global north and the global south.

2.1. GLOBAL DIGITAL DIVIDE

One of the most significant issues the world is currently experiencing is inequality, and there are substantial concerns about the extent to which the advancement of technology is contributing to it. The capacity of new technologies to promote sustainable development is only feasible if all individuals have access to them. Unfortunately, emerging technologies are fostering a new digital divide and all kinds of inequity.[18]

The global digital divide refers to the significant disparities in access to and use of digital technologies between the Global South and the Global North. While the Global North enjoys widespread internet connectivity, advanced infrastructure, and technological advancements, the Global South continues to face substantial barriers that impede their digital participation.

In developed countries, approximately 80 to 90 percent of people have access to the Internet, compared to the least developed countries (LDCs) and landlocked

[18] United Nations Department of Economic and Social Affairs (UN-DESA), 'World Social Report 2020: Inequality in a rapidly changing world.' (2020) <https://www.un.org/development/desa/dspd/wp-content/uploads/sites/22/2020/02/World-Social-Report2020-FullReport.pdf> accessed on 30 June 2023.

developing countries (LLDCs), where only 36 per cent of the population is currently online.[19]

Given the competitive advantage that 'first movers' enjoy in numerous fields related to new technology, it matters how quickly diffusion occurs, and accessibility problems may further disadvantage underdeveloped countries and disadvantaged groups.

If governments and leading corporations, which are frequently based in prosperous countries, fail to lower barriers to the introduction and dissemination of such developments, many of the benefits arising from new technology that developing countries might benefit from may not materialise.

The digital divide, which encompasses countries, regions, communities, people, etc. who are altogether or substantially excluded from the advantages of digital technology, has served as the primary lens for analysing the relationship between digital advancement and inequality.[20]

Comparatively, in Europe and the Americas, around 90% of the general population has internet access, which is nearing 'universal access', determined for practical reasons to be a penetration rate of the Internet of at least 95%, while the average user in Africa is only 40% of the population.[21]

2.1.1 CAUSES OF THE GLOBAL DIGITAL DIVIDE

The disparity in access to digital resources and technology across various nations, regions, and communities is known as the "global digital divide." Disparities in connectivity, cost, infrastructure, and digital literacy are some of the factors influencing this divide. To address the problem and strive towards closing the global digital gap, it is crucial to comprehend these factors.

1. Economic factors: The digital gap is significantly influenced by economic considerations. The financial resources required for investing in digital infrastructure

[19] International Telecommunication Union (ITU) statistics, 'Measuring Digital Development: Facts and Figures.' (2022) <https://www.itu.int/itu-d/reports/statistics/2022/11/24/ff22-internet-use/> accessed 30 June 2023.
[20] Jan van Djik, *The Digital Divide* (Cambridge, Polity Press 2020).
[21] International Telecommunication Union (ITU) statistics, 'Measuring Digital Development: Facts and Figures.' (2022) <https://www.itu.int/itu-d/reports/statistics/2022/11/24/ff22-internet-use/> accessed 30 June 2023.

and achieving ubiquitous connectivity are frequently lacking in low-income nations and marginalised populations. Particularly in rural or isolated places, the cost of constructing and maintaining the essential infrastructure for telecommunications, which includes broadband networks and cellular towers, can be exorbitantly expensive. The difference is exacerbated by people's inability to buy digital gadgets and internet connectivity due to limited financial means.

2. Geographic factors: Geographical restrictions exacerbate the digital gap globally. Due to natural obstacles like mountains, deserts, or deep woods, digital networks are difficult to access in remote or rural areas. It is less appealing for companies that provide services to make an investment in connection since building physical infrastructure is expensive and there aren't many feasible business models there. As a result, residents of these areas frequently have little or no accessibility to digital services, which furthers the gap.

3. Socio-Cultural factors: The global digital gap is also influenced by social and cultural factors. Due to societal conventions, discriminatory practises, and a lack of empowerment, women and girls frequently have limited access to digital resources. Gender inequality is a key hurdle in this regard. Prospects for learning, job opportunities, and engagement in the digital marketplace are constrained by this gender divide. Furthermore, people's capacity to use digital technology and traverse the online world is hampered by low levels of digital literacy, particularly among older people and underserved communities.

4. Lack of Infrastructure: The global digital divide is largely due to a lack of adequate digital infrastructure. Many areas, particularly in developing nations, lack the infrastructure required to set up dependable and affordable connectivity. Broadband networks, mobile coverage, and internet service providers are all included in this. Lack of a sufficient infrastructure limits people's access to digital resources like online educational materials, e-commerce websites, and telehealth services, making it difficult for them to take advantage of the opportunities offered by the digital age.

5. Affordability: Bridging the digital gap is significantly hampered by the prohibitively expensive nature of digital gadgets and internet connectivity. The majority of people in many developing nations cannot afford the price of cell phones, computers, and other digital gadgets. Additionally, low-income people and families

may find the expenses of data plans and internet connections to be exorbitant. As a result, for underserved groups, affordability emerges as a significant barrier to effective access and use of digital technology.

It is essential to address these factors if we are to close the global digital gap. Work to create an increasingly equitable and inclusive global digital economy where individuals and societies have equal opportunity to engage in the digital age, irrespective of their location or socioeconomic status, by comprehending and resolving these reasons.

2.1.2. CHALLENGES IN BRIDGING THE GLOBAL DIGITAL DIVIDE

The endeavour of reducing the global digital gap is one that requires overcoming several obstacles. While providing all people and communities with equal access to digital resources and technology is the aim, there are several challenges that must be overcome to realise this goal. Below are a few of the main challenges facing closing the digital gap worldwide:

1. Infrastructure Creation: Building digital infrastructure is one of the biggest obstacles to closing the digital gap. Especially in developing nations, expanding connections to isolated and neglected areas may be expensive and logistically difficult. It takes a lot of money to build and maintain broadband networks, cell towers, and internet infrastructure; hence, it might not be feasible for service providers to expand their networks to places with low population densities. Physical infrastructure development in some areas is further complicated by topographical obstacles like terrain such as deserts, mountains, or dense woods.

2. Affordability: One of the main obstacles to closing the digital gap is the expensive nature of digital services and internet connectivity. Many people and communities, especially in developing nations, lack access to mobile devices, computers, and other essential digital tools. Additionally, marginalised communities may not be able to afford the expenses of data packages and internet connections. Innovative strategies, such as grants, regulations, and public-private partnerships to encourage competition and drive down costs, are needed to reduce the expense of digital devices and internet access.

3. Digital Literacy and Expertise Gap: The dearth of digital knowledge and abilities presents another major obstacle to closing the digital gap. Many people, especially those living in underprivileged areas, lack the skills necessary to utilise digital devices and traverse the internet. To provide people with the ability to access and use digital resources, digital literacy programmes and initiatives are crucial. These courses must emphasise not only fundamental technological literacy but also more sophisticated abilities, including critical thinking, internet safety, and information assessment.

4. Linguistic and cultural challenges: Building an inclusive digital space necessitates navigating linguistic and cultural obstacles. The internet functions primarily in a small number of major languages, providing a communication barrier for groups who speak indigenous languages and non-English languages. To enable people to access resources and knowledge in their native languages, regional services and content in diverse languages must be created and promoted. In addition, cultural norms and circumstances might affect how people accept and use digital technology. To promote equality in access to and use of digital technology, it is critical to recognise and overcome these cultural obstacles.

5. Relevance and Localization of Digital Material: To close the digital gap, it is also necessary to make sure that digital material is both relevant and localised. To address the unique requirements, circumstances, and cultures of varied populations, information and resources must be modified. This comprises educational resources that have been localised, content that is culturally suitable, and services that take into account the particular difficulties and possibilities that various groups and areas experience. Digital technology may become more usable and relevant for people and communities by emphasising content relevance and localization.

6. Socio-Economic Inequalities: The digital gap is closely related to socio-economic inequality. To effectively bridge the gap, socio-economic inequalities must be addressed. Social exclusion, financial inequality, and poverty restrict people's access to and use of digital technology. Broader socio-economic development measures that advance healthcare, education, and employment prospects must be implemented in tandem with initiatives to close the digital gap. The advantages of digital inclusion are maximised and sustained thanks to this all-encompassing strategy.

In conclusion, there are several obstacles to closing the global digital gap, including the need for infrastructure development, cost, digital literacy, language and cultural hurdles, the relevancy of content, and socioeconomic inequities. It takes a multifaceted strategy to address these issues, including infrastructure improvements, cost-cutting legislation, digital literacy initiatives, content localisation, and inclusive socioeconomic development plans.

2.2. DIGITAL COLONIALISM

Although the use of technological devices and online connectivity has significantly increased globally, debates regarding topics like surveillance, confidentiality, and internet independence frequently frame themselves from the perspective of user behaviour in Western contexts, which may contribute to the propagation of "new kinds of market governance over the informal poor, modifying their habits, social practises, and fiscal policies beneath the guise of poverty reduction."[22]

The gap that separates data-rich and data-poor states is widening on an international level. A small number of corporations have the chance to turn raw data from services supplied in the Global South into value-added data assets due to their concentration in data-driven markets. These services and products create more data, sustaining their competitive advantage.

The gathering and analysis of data is an integral part of many services and products in the modern digital world. The customer's behaviour, tastes, trends, and a number of other factors can all be understood better with the use of this data.

When certain products or services produce more data, it indicates that they are more capable to acquire more information about their consumers or clients. These services and products can improve their features, hone their offerings, and more closely target their marketing campaigns by gaining access to more data. They have an enhanced understanding of their target audience and are better able to make decisions as a result, which could provide them a competitive advantage.

Furthermore, this advantage becomes self-reinforcing or perpetuating. As these products and services continue to gather more data, they gain even more insights and

[22] Payal Arora, 'The Bottom of the Data Pyramid: Big Data and the Global South' (2016) 10 International Journal of Communication.

information, enabling them to stay ahead of their competitors. This cycle creates a feedback loop where the accumulation of data strengthens their market position and gives them a continuous advantage.

At present, data may not yet be regarded as a resource in developing states, and policymakers may not know how to safeguard the interests of citizens without having a deeper knowledge of the economic and political implications of data.[23] This has been characterised as a new form of colonialism known as 'digital colonialism', as "knowledge, authority, and power to sort, categorise, and order human activity rests with the technologist, for whom (populations of the Global South) are merely data-producing 'human natural resources'".[24]

Presently, there is no single universally accepted definition of 'digital colonialism.' The term emerged as a concept to describe the power dynamics and imbalances between dominant entities, often from developed countries, and the exploitation of data from less powerful countries or marginalized communities. It draws parallels to historical colonialism, where resources and labour were extracted from colonized regions for the benefit of colonizers.

While there is no standardised definition, 'digital colonialism' generally refers to the extraction, control, and exploitation of data, often by large corporations or powerful nations, leading to the marginalisation and disempowerment of individuals, communities, or countries whose data is being exploited. It highlights concerns about the concentration of power, surveillance, privacy infringement, and the potential reinforcement of existing inequalities in the digital era.

Herbert Schiller, an American media critic and scholar, as documented in his 1976 text 'Communication and Cultural Domination'[25], did not specifically address the concept of "digital colonialism". However, his ideas and theories on media imperialism and cultural dominance can be related to the broader discussion of digital colonialism.

---

[23] Susan Ariel Aaronson, 'Data Is a Development Issue' (2019) Centre for International Governance Innovation (CIGI) Papers, No. 223 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3589827> accessed 30 June 2023.

[24] Abeba Birhane, 'Algorithmic Colonisation of Africa' (*The Elephant*, 21 August 2020) <https://www.theelephant.info/long-reads/2020/08/21/algorithmic-colonisation-of-africa/> accessed 30 June 2023.

[25] Herbert Schiller, *Communication and Cultural Domination* (International Arts and Sciences Press 1976).

Schiller's work primarily focused on the role of multinational corporations, particularly those based in the United States, in shaping and controlling global media and communication systems. He argued that these corporations, through their dominance of the media and cultural industries, exerted a form of cultural imperialism on other nations, imposing Western values and perspectives while undermining local cultures and media industries.

While Schiller's analysis predates the widespread advent of digital technologies, many of his ideas can be applied to the contemporary issue of digital colonialism. Digital colonialism refers to the unequal power dynamics and control exerted by Western technology companies, particularly those from the United States of America and Europe, over the digital infrastructure, data, and information flows of developing countries.

Schiller's concerns about the concentration of media power in the hands of a few corporations and the potential erasure of local cultures can be extended to digital platforms and the potential loss of digital sovereignty experienced by many countries. His work underscores the need for critical examination and resistance against the hegemony and domination facilitated by digital technologies and the global media landscape.

Nick Couldry and Ulises A. Mejias define 'data colonialism' as a concept that refers to the exploitation and domination of individuals and societies through the extraction, control, and commodification of data.[26] They argue that data colonialism is an extension of historical colonialism, where power and control are exercised over people's data, enabling the concentration of wealth and power in the hands of a few dominant entities.

According to Couldry and Mejias, data colonialism involves the appropriation of data from individuals and communities without their informed consent or understanding of the implications. This data is often extracted through surveillance technologies, social media platforms, and other digital services that collect vast amounts of personal information. These entities, which they refer to as 'data empires,' amass immense wealth and influence by monetizing and leveraging the data they collect.

[26] Nick Couldry and Ulises A. Mejias, *The Costs of Connection: How Data is Colonising Human Life and Appropriating It for Capitalism* (Stanford University Press 2019)

Data colonialism also perpetuates existing power imbalances and reinforces social inequalities. Couldry and Mejias argue that data empires exert control over people's lives by shaping their behaviour, decisions, and opportunities based on the analysis of their data. This control can be seen in targeted advertising, personalized content recommendations, and algorithmic decision-making, which can reinforce existing biases and marginalize certain individuals and groups. They argue that it is crucial to challenge data colonialism and establish alternative models that prioritize data sovereignty, ethical data practices, and the redistribution of power and benefits associated with data.

According to University of Copenhagen professors Marker, Vestergaard, and Hendricks, 'Digital colonialism' is the decentralised gathering and administration of digital information from individuals with or without their explicit consent through communication networks created and operated by multinational technology companies.[27]

According to University of Copenhagen professors Marker, Vestergaard, and Hendricks the structure of 'digital colonialism' has four primary actors[28]:

(1) The western technology companies that develop and offer the infrastructure and technology for gathering data for advertisement targeting and distribution;

(2) The advertising and consulting companies that utilise the data supplied by technology companies to target different groups with highly individualised advertisements and personalised messages in an effort to increase profits;

(3) The regional businesses, political parties, and various local organisations that employ these advertising and consulting companies to assist them in imposing their different agendas and propagandas for their respective areas;

(4) Individuals who, deliberately or inadvertently, serve as target audiences for regional businesses, political parties, and local organisations, as well as sources of data for tech corporations.

2.2.2. DIGITAL COLONIALISM VS DIGITAL SOVEREIGNTY

[27] Silas L. Marker, Mads Verstergaard and Vincent F. Hendricks, 'Digital Colonialism on the African Continent' (2019) IOL Business Report <https://www.iol.co.za/business-report/opinion/opinion-digital-colonialism-on-the-african-continent-17493010> accessed on 30 June 2023.
[28] ibid.

Data sovereignty and data colonialism are two concepts that address the ownership, control, and use of data. While data sovereignty refers to the rights of individuals, organizations, or governments to exercise control over their own data, data colonialism refers to the exploitation and domination of data by powerful entities, often from developed countries, at the expense of less powerful ones.

'Digital sovereignty' refers to the ability of a nation or an individual to exercise control and authority over their digital activities, data, and infrastructure within their jurisdiction. It encompasses the concept of maintaining autonomy, independence, and security in the digital realm, free from external influences or dominance. In an increasingly interconnected and data-driven world, digital sovereignty has become a crucial aspect of national security, economic development, and the protection of individual rights.

At its core, digital sovereignty entails the ability of a nation to shape and regulate its digital ecosystem according to its own laws, values, and interests. This includes the establishment of policies, regulations, and technical standards that govern data privacy, cybersecurity, intellectual property rights, and access to digital services. By exercising digital sovereignty, nations can safeguard their citizens' privacy, protect critical infrastructure, and promote fair competition in the digital marketplace.

One key aspect of digital sovereignty is data sovereignty, which refers to the control and ownership of data generated within a nation's borders. Data sovereignty asserts that data collected within a jurisdiction should be subject to the laws and regulations of that jurisdiction, and should not be subject to unrestricted access or exploitation by foreign entities. Data localization measures, such as requiring data to be stored locally or imposing restrictions on cross-border data transfers, are often implemented to ensure data sovereignty.

Another important element of digital sovereignty is technological independence. This entails reducing dependency on foreign technologies and fostering the development of indigenous technological capabilities. It involves promoting domestic research and development, nurturing local technology start-ups, and investing in critical digital infrastructure. By reducing reliance on foreign technologies, nations can mitigate the risks associated with external control or manipulation of their digital systems.

Digital sovereignty also encompasses issues of internet governance. It involves advocating for a more inclusive and equitable global digital governance framework that respects the principles of national sovereignty and ensures equal participation of all stakeholders. This includes promoting multi-stakeholder approaches that involve governments, civil society, private sector entities, and technical experts in decision-making processes related to internet governance.

Achieving digital sovereignty does not imply isolation or complete detachment from the global digital landscape. It recognizes the importance of international cooperation, collaboration, and exchange of knowledge and expertise. However, it emphasizes the need for a balanced approach that safeguards national interests and values while participating in global digital networks.

The concept of digital sovereignty is gaining prominence as nations grapple with the challenges posed by the increasing influence of multinational technology companies, cybersecurity threats, data breaches, and privacy concerns. It has significant implications for national security, economic competitiveness, and the protection of individual rights in the digital age.

Fundamentally, digital colonialism threatens a state's sovereignty by allowing large tech companies to exploit the data of different countries, regulate every bit of data that is available to them, and take an active and integral role in their internal affairs. The greatest threat posed by 'data colonialism' is that a country, despite being technically independent, could become entirely dependent on the technological facilities and systems of big tech companies in the Global North and turn into another source of revenue for these corporations. This would transform the country into a 'colony' of big tech companies, with their country of origin becoming a Global North country, both metaphorically and literally.

Essentially, data colonialism places Global South country at the mercy of a few large foreign technology companies that have influence over its digital economy and, in turn, the Global North country that represents these companies.[29] Data sovereignty can counter data colonialism in several ways:

[29] Sarah A. Paco, 'Data Colonialism, the Danger It Poses to India's Democracy, and the Effectiveness of Data Localization Laws as Resistance.' (2022) 48 Rutgers Computer & Tech LJ 254.

1. Ownership and Control: Data sovereignty emphasizes the idea that data belongs to the individuals or organizations that generate it. It asserts the rights of data creators to retain ownership and control over their data. By exercising sovereignty over their data, individuals and organizations can resist attempts by external entities to exploit or dominate their data.

2. Legal Frameworks: Data sovereignty is often supported by legal frameworks and regulations that protect data and ensure its controlled use. These frameworks can include data protection laws, privacy regulations, and intellectual property rights, among others. Such regulations aim to prevent the unauthorized collection, use, or exploitation of data by external entities, thereby countering data colonialism.

3. Local Data Infrastructure: Data sovereignty promotes the development of local data infrastructure, including data centres, networks, and cloud services, to store and process data within the jurisdiction of the data owner. By establishing local infrastructure, countries and organizations can reduce dependence on external entities for data storage and processing, reducing the risk of data colonialism.

4. Data Localization: Data sovereignty often encourages data localization, which refers to the requirement or preference for data to be stored and processed within a specific geographical location or jurisdiction. Data localization policies can enhance data sovereignty by ensuring that data remains within the control of the country or organization that generated it, making it harder for external entities to exploit or extract value from the data without permission.

5. Empowerment and Collaboration: Data sovereignty promotes the empowerment of individuals, organizations, and governments to make informed decisions about their data. It encourages collaboration among different stakeholders to develop data governance frameworks that protect the interests and rights of data creators. By empowering and collaborating with local actors, data sovereignty helps to counter the power dynamics inherent in data colonialism.

It’s worth noting that data sovereignty and data colonialism are complex issues, and their relationship is multifaceted. While data sovereignty can act as a countermeasure to data colonialism, achieving a fair and equitable data landscape requires broader efforts, such as international cooperation, ethical data practices, and addressing the underlying power imbalances in the global data ecosystem.

2.3. SURVEILLANCE CAPITALISM

Both descriptive and critical analyses that label the current digital political-economic system as informational capitalism place a significant emphasis on data. Informational capitalism is a method of production that is primarily focused on extracting and analysing information to extract and build wealth. It is also known as surveillance capitalism and data capitalism. This converts information—especially information in the form of data that is machine readable—into a crucial economic resource.[30]

'Surveillance capitalism' is a term coined by Shoshana Zuboff, a renowned American scholar and Harvard professor, to describe the economic system that has emerged with the rise of digital technology and the internet. In her seminal book, Zuboff outlines the profound impact of this new form of capitalism on society, individual autonomy, and democracy.[31]

At its core, surveillance capitalism is characterized by the extraction, analysis, and commodification of vast amounts of personal data from individuals as they navigate the digital realm. This data is harvested through various means, such as online searches, social media interactions, and smartphone usage, and is then repurposed to create highly detailed profiles of individual's behaviour, preferences, and interests.

The accumulation of this personal data enables surveillance capitalists, typically tech companies and digital platforms, to generate unprecedented insights into human behaviour. These insights, in turn, fuel the development of sophisticated prediction algorithms and targeted advertising systems, which are leveraged to influence individuals' choices and shape their behaviour.

One of the key elements of surveillance capitalism is its focus on the future. Instead of simply analysing past behaviour, it aims to predict and shape future behaviour. This predictive power allows surveillance capitalists to not only anticipate individual preferences and needs but also manipulate them through personalized advertisements, recommendation systems, and other targeted interventions. This process creates a feedback loop wherein individuals' data is continuously harvested and used to refine and optimize the algorithms and systems employed by surveillance capitalists.

---

[30] Julie E. Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (Oxford University Press 2019)

[31] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile Books England 2019)

Zuboff argues that surveillance capitalism represents a fundamental shift in the capitalist logic.[32] Traditionally, capitalism relied on the extraction of value from nature or human labour. However, in surveillance capitalism, the primary source of value extraction is human experience and behaviour. This new form of capitalism treats human life as a marketable commodity, transforming individuals into passive sources of data to be kept under surveillance, analysed, and monetized.

Furthermore, surveillance capitalism has profound societal implications. It erodes individual autonomy and privacy, as personal data is collected and exploited without individuals' fully informed consent. The pervasive surveillance and manipulation of individuals' choices also undermine the democratic principles of freedom and self-determination. This new economic logic threatens to turn individuals into mere instruments of profit, subverting the very foundations of a democratic society.

Moreover, surveillance capitalism contributes to the consolidation of power and wealth in the hands of a few dominant tech companies. These companies, armed with vast amounts of personal data, have a significant advantage over competitors and can exert immense influence over markets, politics, and public discourse. The resulting power asymmetry exacerbates existing inequalities and undermines fair competition and innovation.

In response to the rise of surveillance capitalism, Zuboff calls for the development of a new social contract that reclaims individual sovereignty over personal data and establishes democratic oversight of data practices. She emphasizes the need for transparency, accountability, and meaningful consent in the collection and use of personal information. Additionally, she advocates for legal and regulatory frameworks that protect individual privacy rights and foster a more equitable distribution of power in the digital age.[33]

2.3.1. SURVEILLANCE CAPITALISM AND BIG DATA

The primary aspect of surveillance capitalism is big data. Corporations and governments are gathering, preserving, and analysing vast centralised databases containing information about internet users worldwide. This provides them the ability

[32] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile Books England 2019)
[33] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile Books England 2019)

to deduce characteristics about individuals, including variables including their sexuality, belief system, drug usage habits, political views, and behavioural patterns, that they would not otherwise share. Then, in order to further corporate profit and governmental dominance, the data is used to control individuals, communities, and organisations.[34]

By nature, big data violates individual privacy. Data miners rely extensively on artificial intelligence to make sense of the enormous data volumes produced. AI often 'learns' by examining vast datasets with the objective of making predictions. When implemented for individuals, it gathers private and archival data to make future predictions. Big Data must draw its projection accuracy from the depth of data that can be gathered about individuals and groups because machines cannot 'think,' which is how it gets its predictive accuracy. Subsequently, enormous amounts of data are required, and widespread surveillance usually becomes essential.[35]

Individuals all across the world are now clients of the state corporate ruling elite from the Global North, given that surveillance is the new revenue model for tech. The overly inclusive term 'big data' has been employed in this arrangement to hide surveillance and monitoring activities. Big data is merely a cover for surveillance when used in relation to people.

Sensitive human information can be extracted and made a profit off of, but the results are vastly different economically and morally than when oil is extracted mechanically. Producing 'ethical big data' for people, as some academics suggest, is like producing 'clean coal' for the environment.

Thus, surveillance capitalism exposes society to an unethical degradation of privacy that disadvantages the Global South. Similar to the rail systems of colonial empires, surveillance capitalists harvest data from the Global South, process it in their metropolitan areas, and then regurgitate it back to the colonised masses in the form of necessary digital services.

[34] Michael Kwet, 'Digital colonialism: US empire and the New Imperialism in the Global South.' (2019) Race & Class 60(4) DOI: 10.1177/0306396818823172 <https://ssrn.com/abstract=3232297> accessed 30 June 2023.
[35] ibid.

The dominance of the Global North in the digital ecosystem on an infrastructure level empowers them to keep authority over the digital society and foster dependency in the Global South while boosting the influence and impact of Big Tech corporations.

2.3.2. SURVEILLANCE CAPITALISM AND SUBJUGATED SOCIETY

The society of subjugation is a specific kind of surveillance society in which the State employs surveillance technologies to create a policing infrastructure intended to police, punish, and eventually eradicate an opposing minority group.[36] In authoritarian states, technological surveillance is used to oppress people along identification lines that go beyond race alone yet still involve it.

For the objective of subjugated society surveillance, subaltern identification includes the following additional categories: race or ethnicity, religion, nationality, political opinion or affiliation, and participation in a social group.[37] Many of the groups targeted by oppressive regimes fall into more than one of the five identity-based categories. A further factor in the subjugated society is 'strategic surveillance' which is used by the State to track and then suppress elements that it perceives as posing a threat to its power.

As usual in subjugated societies, regulation is created by transforming individuals into limitless data sources. The primary objective of distributing this data to corporations is to increase revenue. Legal studies on digital surveillance and big data policing mostly examine control societies, particularly wherein the State works with corporate interests to develop cutting-edge surveillance methods.[38] The state, which has unrestricted jurisdiction over the implementation of surveillance, its scope, and its intrusion into the lives of targeted individuals, is the primary beneficiary of surveillance and the creator of policy in the subjugated society.

In four significant ways, the subjugated society broadens academic knowledge of digital surveillance; First, it demonstrates how identification indicators other than race

[36] Khaled Ali Beydoun, 'The New State of Surveillance: Societies of Subjugation' (2022) 79(2) Washington & Lee Law Review.
[37] Christopher C. Malwitz, 'Particular Social Groups: Vague Definitions and an Indeterminate Future for Asylum Seekers' (2018) 83(3) Brooklyn Law Review.
[38] Tom Wheeler, Phil Verveer, and Gene Kimmelman, 'The need for regulation of big tech beyond antitrust' (*Brookings*, 23 September 2020) <https://www.brookings.edu/blog/techtank/2020/09/23/the-need-for-regulation-of-big-tech-beyond-antitrust/> accessed 30 June 2023.

may be the main justification for monitoring in other countries, like Uganda, where sexual minorities are the primary targets of surveillance,[39] or like Egypt, a country with a majority of Muslims, the Sisi administration has targeted the Muslim Brotherhood, a global political movement seen as the regime's biggest threat, with its digital surveillance programme.[40]

Second, digital surveillance technology deployment in authoritarian regimes is frequently intended to discriminate along identity lines rather than just cause disproportionate effects along identity lines. To further the effectiveness of its surveillance, the State engages in even more ominous relationships with corporations to create technology that isolate and identify the distinctive physical traits of ethnic minorities, for example the Uyghur.[41] In addition to racial prejudices included in algorithmic code, Chinese digital surveillance technologies are designed particularly to separate Uyghur, Tibetan, and other minority ethnic groups from the majority Han.

Third, a key contrast between control and subjugated societies is the ability to resist surveillance. In the former, activists have used 'sousveillance,' a technique in which people use their technology, most notably their smartphones, to record and subsequently spread evidence of governmental brutality and overreach.[42] In subjugated societies, this method of surveillance resistance, along with others like "using umbrellas to cover individual's facial features," "spray painting over the lenses of facial identification cameras," or "putting on face paint to deceive cameras," would be severely punished, so in regard to this state response, it is completely avoided.[43]

Fourth, the impact of digital monitoring in authoritarian states is different from how it operates in democratic ones. In place of possessing citizenship and the array of

[39] Human Rights Watch, 'Uganda: Stop Police Harassment of LGBT People.' (*Human Rights Watch*, 17 November 2019) <https://www.hrw.org/news/2019/11/17/uganda-stop-police-harassment-lgbt-people> accessed 30 June 2023.
[40] Ashraf El-Sherif, 'The Egyptian Muslim Brotherhood's Failures' (*Carnegie Endowment for International Peace*, 01 July 2014) <https://carnegieendowment.org/2014/07/01/egyptian-muslim-brotherhood-s-failures-pub-56046> accessed 30 June 2023.
[41] Drew Harwell and Eva Dou, 'Huawei tested AI software that could recognize Uighur minorities and alert police, report says.' (*The Washington Post*, 8 December 2020) <https://www.washingtonpost.com/technology/2020/12/08/huawei-tested-ai-software-that-could-recognize-uighur-minorities-alert-police-report-says/> accessed 30 June 2023.
[42] Steve Mann, 'Veilance and reciprocal transparency: Surveillance versus sousveillance, AR glass, lifeglogging, and wearable computing' (2013) IEEE International Symposium on Technology and Society (ISTAS): Social Implications of Wearable Computing and Augmediated Reality in Everyday Life, Toronto, ON, Canada, 2013. DOI:10.1109/ISTAS.2013.6613094.
[43] Chaz Arnett, 'Race, Surveillance, Resistance.' (2020) 81(6) Ohio State Law Journal 1103-1142.

constitutional rights that arise from it, individuals in authoritarian states are given very little security and privacy from the power of surveillance, or, as demonstrated by the hardships of the Uyghur in Xinjiang, none at all.[44]

While legal scholars protest the increasing prevalence of authoritarian practises in democracies, particularly in the context of the expansion of surveillance throughout the worldwide "War on Terror," subjugated societies are unrestrained in their use of technologies for surveillance to punish their opponents and solidify their power.[45] Democratic control societies are constrained by public and legal scrutiny on excessive surveillance, at least on the surface. While it is nonetheless "crucial for the system to preserve the illusion of liberty and privacy" such illusions do not exist in subjugated societies.

[44] Sean R. Roberts, *The War on the Uyghurs: China's Internal Campaign against a Muslim Minority* (Princeton University Press 2020)

[45] Henry A. Giroux, 'Totalitarian Paranoia in the Post-Orwellian Surveillance State.' (2015) 29(2) Cultural Studies, Routledge, Taylor and Francis Group.

CHAPTER 3

ROLE OF MULTINATIONAL CORPORATIONS IN DIGITAL COLONIALISM AND SURVEILLANCE CAPITALISM

The concepts of digital colonialism and surveillance capitalism are significantly influenced by multinational corporations and technology companies. These two ideas are related and have significant effects on society, the economy, and personal privacy.

The control and use of digital platforms, data, and infrastructure by large multinational corporations, many of which have their headquarters in countries with advanced economies, is referred to as "digital colonialism." These corporations exercise influence over the digital environments of less developed countries by utilising their technological strength and worldwide reach. This control frequently leads to dependence in the economy, culture, and politics, much like the previous colonial linkages.

The two main players in this process are multinational corporations and technological companies. They have the assets, know-how, and market access required to achieve and sustain digital supremacy. In emerging economies, they construct and maintain the digital infrastructure, including the networks of telecommunications and data centres. They do this to restrict accessibility to digital services and to regulate the flow of information, frequently to their own advantage.

The economic paradigm known as "surveillance capitalism" allows corporations to amass enormous quantities of private and confidential data via digital surveillance and to monetize it for things like targeted advertising.

When it comes to gathering, analysing, and using user data, technology companies are at the forerunners of this data-driven economy. These companies entice customers to reveal personal information and interact with their platforms by providing free or inexpensive digital services. The information gathered is then utilised to develop comprehensive profiles of people, allowing for accurate ad targeting and influencing user behaviour.

Technology companies make large revenues from this process, which acts as a strong financial incentive for the growth and escalation of surveillance methods. Due to their widespread worldwide presence, multinational corporations, particularly the digital giants, are important participants in surveillance capitalism. Since billions of people use their platforms and services globally, they can gather enormous amounts of data. Transcending national lines, this data collecting raises issues of privacy, permission, and the concentration of control in the hands of a few powerful companies.

The impact of multinational corporations and technology companies' participation in surveillance capitalism and digital colonialism on society is significant. First, because less-developed countries are dependent on foreign firms for their technological infrastructure and access to digital services, digital colonialism worsens existing economic inequality throughout the world. This dependence stifles regional economic growth and maintains existing power disparities.

Second, the commercialization and extraction of personal data under surveillance capitalism raises questions about invasions of privacy and informed consent. The massive gathering and analysis of user data raises ethical and legal concerns since people frequently have little control over their data and how it is used.

Targeted advertising and algorithmic manipulation used by surveillance capitalism may also have a big impact on user behaviour, preferences, and viewpoints. This may intensify filter bubbles, encourage political polarisation, and aid in the dissemination of false information, all of which have serious ramifications for democracy.

Furthermore, the concentration of control in the digital world is a worry due to the dominance of a handful of multinational corporations and technological companies. These corporations have enormous power and access to a wealth of data, which might undermine competition, stifle innovation, and jeopardise democratic decision-making processes.

3.1. THE DIGITAL ECONOMY

A system of economics that is predominantly focused on digital platforms and technology is referred to as the "digital economy." It includes the creation, provision, and use of products and services that significantly rely on digital technologies like the internet, mobile phones, and other gadgets. E-commerce, electronic payment systems,

online products and services, developing software, digital advertising, and other industries are all part of the digital economy.

To produce, distribute, and consume products and services, the digital economy significantly relies on digital platforms and technology. It includes a broad spectrum of industries and pursuits that have undergone a digital transformation. Following are a few examples of the various kinds of digital economy aspects:

1. E-commerce: Online merchants like Amazon and Alibaba have revolutionised consumer purchasing behaviour. Online shopping allows customers to explore and buy things that are then delivered right to their homes. E-commerce gives corporations access to a worldwide clientele and facilitates and speeds up the purchasing process.

2. Digital payments: Platforms for mobile payments (such as Apple Pay and Google Pay) as well as services like PayPal and Venmo have completely transformed how people conduct financial transactions. Without using actual currency or conventional banking systems, they offer safe and practical ways to make payments, move money, and manage personal accounts.

3. Online services: By linking people who offer services with those who need them, companies like Airbnb, Uber, and Upwork have challenged established sectors. These online marketplaces use digital technology to enable peer-to-peer exchanges for things like lodging, transportation, and freelance employment.

4. Digital Content and Media: The entertainment sector has been entirely transformed by online streaming services like Netflix, Spotify, and YouTube. They offer on-demand access to a variety of digital media, such as videos, music, and movies. Through the use of these platforms, consumers are now less likely to use tangible formats like CDs and DVDs for consuming and distributing material.

5. Software Development: The production of programmes, games, and software solutions for a variety of companies is a major component of the digital economy. Digital tools and software applications are created and provided by businesses like Microsoft, Adobe, and Salesforce to boost productivity, efficiency, and creativity in a variety of industries.

6. Digital advertising and marketing: Targeted advertising is made possible by online advertising platforms like Google Ads and Facebook Ads. Companies are now required to employ digital marketing tactics, such as search engine optimisation (SEO), social media marketing, and content marketing, to advertise their goods and services online.

7. Data analytics and artificial intelligence (AI): Companies use data analytics and AI technology to gather insights, enhance decision-making, and personalise consumer experiences. The digital economy creates enormous volumes of data. Examples include the machine learning algorithms used in fields including banking, healthcare, and e-commerce, as well as recommendation systems, predictive analytics, and others.

8. Internet of Things (IoT): The IoT is a term used to describe a network of linked objects that interact and gather data. Process automation and optimisation are made possible by IoT technology in sectors including manufacturing, transportation, and agriculture. The development of the digital economy is aided by connected devices, including industrial sensors, smart appliances, and wearable technology.

3.2. ROLE OF MULTINATIONAL CORPORATIONS IN THE DIGITAL ECONOMY

Global corporations and technology firms are essential components of the digital economy and get several benefits from its transformative potential. First, by utilising online platforms, companies may grow their operations and establish connections with clients all over the world. For instance, businesses like Amazon and Alibaba have created online markets to help with international trading.

Second, digital technology helps these companies operate more efficiently. They improve several facets of their organisation, including supply chain management and customer assistance, by automating procedures, using data analytics, and utilising artificial intelligence (AI). This effectiveness is demonstrated by Google's use of AI algorithms for targeted advertising.

Additionally, via digital advancements, multinational corporations and technology companies spur innovation and disrupt traditional sectors. They drive technical advancement by constantly creating new goods, services, and business models. Companies like Tesla and Airbnb, which provide electric automobiles and online

marketplaces for lodging, have revolutionised their respective sectors. These businesses use the massive volumes of data produced by the digital economy to gain insights and make decisions. They may customise services, enhance client experiences, and make strategic choices by analysing consumer behaviour and preferences. A good example of this data-driven strategy is Facebook's use of user data for targeted advertising.

Moreover, these companies promote collaborative ecosystems by joining up with various organisations to utilise their complementary resources and skills. They build value-added services, increase the range of their product offerings, and develop novel solutions through collaborations. This ecosystem is shown by Microsoft's partnerships with technology companies to provide integrated solutions on the Azure cloud platform.

The digital economy also creates new revenue streams. Through a variety of digital business models, including subscription-based services, online advertising, e-commerce platforms, and the distribution of digital content, multinational businesses and technology companies make money. The success of Netflix as a subscription-based streaming service serves as an example of this revenue potential.

To summarise, the digital economy has a substantial beneficial effect on multinational corporations and technological companies. They take make use of its worldwide reach, increase efficiency through automation and analytics, promote partnerships, drive innovation and disruption, and investigate other income streams. These corporations influence the future of the global economy as leaders in the age of digitization.

3.3. INFLUENCE OF MULTINATIONAL CORPORATIONS ON DIGITAL COLONIALISM AND SURVEILLANCE CAPITALISM

In today's globalised society, multinational companies (MNCs) have emerged as strong forces that operate across borders and have a substantial impact on a variety of societal facets. Concerns have been voiced recently regarding MNC influence in the fields of surveillance capitalism and digital colonialism. This refers to the methods used by MNCs, particularly those operating in the technology sector, to exert control over data, extract revenue from it, and reshape social and political environments.

Digital colonialism refers to the idea that dominant multinational corporations from developed countries, primarily those with headquarters in Global North countries, such as Silicon Valley in the United States of America, exercise a kind of digital supremacy over less developed countries. These businesses have unprecedented access to enormous volumes of user data through the provision of digital services, platforms, and infrastructure, which they use to strengthen their market positions and influence digital ecosystems.

Concerns about the loss of local autonomy, economic reliance, and the possibility of cultural homogenization are raised by this supremacy. On the other hand, surveillance capitalism refers to the monetization of personal information for reasons such as targeted advertising. MNCs gather a lot of consumer information via a variety of channels, such as social networking sites, internet searches, and linked products.

The subsequent analysis, processing, and sale of this data to marketers creates an environment in which people's actions and preferences are continuously tracked and compensated. The model of surveillance capitalism is criticised for violating privacy rights, undermining democracy, and sustaining socioeconomic inequality.

The impact of MNCs on surveillance capitalism and digital colonialism is substantial. In terms of the economy, they gain great wealth and influence by reshaping markets and influencing politics and policy. Socially, they have the power to worsen current inequities by influencing public opinion and defining cultural norms. Concerns about the concentration of power, the capacity to sway information flows, and the potential to sculpt political narratives are raised politically.

Through their data-centric business strategies and technological developments, companies like those in the United States of America like Apple, Google, Amazon, Netflix, Microsoft, and Facebook; Europe with Mimecast and Spotify; and China with TikTok and Alibaba certainly wield significant economic and political influence.[46]

It is therefore essential to learn about some of these globally recognised corporations to comprehend the ramifications of their impact on digital colonialism and surveillance capitalism, which include the Big Five American technological

[46] Gyanda Kakar, 'Cognitive Dysphoria: Evaluating the Paradigm Shift of Artificial Intelligence Technology in Digital Colonialism' (2021) 2 Indian J Artificial Intel & L 7

corporations: Alphabet (Google's parent company), Amazon, Apple, Meta (formerly Facebook Inc.), and Microsoft.

3.3.1. ALPHABET INC.

Google's parent company and global corporation, Alphabet Inc., was established in 2015.[47] It was developed because of Google's organisational restructuring, which allowed the corporation to distinguish between its more experimental projects and its essential internet services. Google is Alphabet's most well-known subsidiary, and it acts as a holding company for a variety of businesses. Technology giant Google, the flagship subsidiary of Alphabet, is well known for its internet-related products and services. With Google Search, it leads the market for search engines. It also provides a wide range of online services, such as Gmail, Google Maps, Google Drive, and YouTube. Google also works on hardware, including the Pixel smartphone, Nest smart home appliances, and the Google Cloud Platform for corporate solutions.[48]

The organisational structure of Alphabet encourages innovation and expansion outside of Google's primary market. It has several subsidiaries, including the self-driving vehicle technology business 'Waymo'[49], the life sciences and healthcare technology company 'Verily'[50], and the artificial intelligence research facility 'DeepMind'[51]. Alphabet investigates cutting-edge technology and forays into new sectors through these organisations.

Given the fact that it runs a variety of platforms and services that amass enormous quantities of user data for the purpose of monetization and control, Alphabet Inc. plays a big role and has a substantial impact on digital colonialism and surveillance capitalism. Large amounts of user information, including search queries, browsing histories, location data, and personal preferences, are gathered by Alphabet Inc. through its subsidiaries, including Google and YouTube.

---

[47] U.S. Securities and Exchange Commission, 'Form 8-K: Current Report Pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934' (2015) <https://www.sec.gov/Archives/edgar/data/1652044/000119312515336577/d82837d8k12b.htm> accessed 30 June 2023.

[48] Google, 'About Google', (2015) <https://about.google/> accessed 30 June 2023.

[49] Waymo, 'Waymo - Autonomous Driving Technology Company' (2016) <https://waymo.com/> accessed 30 June 2023.

[50] Verily Life Sciences LLC, 'Verily: Home' (2015) <https://verily.com/> accessed 30 June 2023.

[51] DeepMind Technologies Limited, 'DeepMind' (2014) <https://www.deepmind.com/> accessed 30 June 2023.

Through targeted advertising and other data-driven services, user profiles may be made in depth using this data. Google's privacy policy outlines the types of data collected and how it is used for personalized advertising.[52]

The dominance of Alphabet Inc. over search engines courtesy of Google and video-sharing websites owing to YouTube gives it substantial influence over the flow of information and access to knowledge. Alphabet Inc. may sway public opinion with this power, manage narratives, and affect user behaviour. Data on the market share of global search engines regularly demonstrates Google's dominance of the search industry.[53] With billions of active users every month and an enormous influence on popular culture, YouTube dominates the industry.

The digital divide between Global North's developed and Global South's developing countries may get worse because of this supremacy. While Alphabet Inc. offers products and services, it also forges dependence and exploitative connections while gaining from the data extraction of users from developing countries.

Substantial privacy and surveillance issues are raised by Alphabet Inc's data collection practises. Individuals' privacy rights may be violated as a result of extensive surveillance and profiling, which also makes it possible for both private and government entities to monitor individuals.[54]

In 2010, it was revealed that Google's Street View vehicles, which took pictures for the mapping service, were also gathering information from unsecured Wi-Fi networks, including users' personal data and browsing history. The scale of Google's data collection practises and their effects on user privacy came under scrutiny because of this occurrence.[55]

It was disclosed in the PRISM case of 2013 that Google took part in a surveillance programme run by the National Security Agency (NSA) that gave access to user

[52] Google Policies, 'Privacy Policy' (15 December 2022) <https://policies.google.com/privacy> accessed 30 June 2023.
[53] StatCounter Global Stats, 'Search Engine Market Share Worldwide' (May 2023) <https://gs.statcounter.com/search-engine-market-share> accessed 30 June 2023.
[54] Douglas C. Schmidt, 'Digital Content Next: Google Data Collection Paper' (21 August 2018) <https://digitalcontentnext.org/wp-content/uploads/2018/08/DCN-Google-Data-Collection-Paper.pdf> accessed 30 June 2023.
[55] Reuters, 'FCC probes Google's Street View data collection' (*Reuters*, 11 November 2010) <https://www.reuters.com/article/google-privacy-idCNN1021543120101110> accessed 30 June 2023.

data.[56] Google claimed they were not directly involved and had not given direct server access. They also claimed they were not aware of PRISM.

Reports, however, claimed the NSA had such access. Google responded with legitimate requests while pursuing legal action to demand greater openness. After that, they strengthened their security procedures. Although Google's role isn't entirely apparent, the case prompted a larger conversation about user data protection, government surveillance, and privacy.[57]

An investigation by the Associated Press in 2018 found that Google continued to monitor users' positions across a number of applications and services even after location history was turned off. This sparked questions regarding the degree of user control over their location data as well as the openness of Google's data collection practises.[58]

Some lawmakers were unconvinced by Google's explanation of how they use location data to improve customer experiences. Sen. Mark Warner of Virginia expressed his displeasure and claimed that technology corporations frequently stray from customer expectations. He urged the adoption of regulations that would give people more power over their data.

Sen. Warner's worries were echoed by New Jersey Rep. Frank Pallone, who advocated for comprehensive legislation to address consumer privacy and data security vulnerabilities. The Associated Press article that revealed Google's use of location history, online and app activity, and device-level location services prompted the senators' comments. The article highlighted the ongoing controversy over user privacy and technology corporations' business practises.[59]

The U.S. Department of Justice (DOJ) brought a landmark antitrust lawsuit against Google Inc., alleging that Google had engaged in anticompetitive behaviour in the

[56] Glenn Greenwald and Ewen MacAskill, 'NSA Prism program taps in to user data of Apple, Google and others.' (*The Guardian*, 7 June 2013) <https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data> accessed 30 June 2023.
[57] Ellen Nakashima, 'NSA surveillance program still raises privacy concerns years after exposure, member of privacy watchdog says.' (*The Washington Post*, 29 June 2021) <https://www.washingtonpost.com/national-security/nsa-surveillance-xkeyscore-privacy/2021/06/29/b2134e7a-d685-11eb-a53a-3b5450fdca7a_story.html> accessed 30 June 2021.
[58] Ryan Nakashima, 'AP Exclusive: Google tracks your movements, like it or not.' (*Associated Press News*, 14 August 2018) <https://apnews.com/article/north-america-science-technology-business-ap-top-news-828aefab64d4411bac257a07c1af0ecb> accessed 30 June 2023.
[59] ibid.

digital search and advertising markets.[60] In this case, a $22.5 million civil penalty judgement and a permanent injunction were approved by the District Court for the Northern District of California. This was the biggest civil penalty in the history of cases filed by the Federal Trade Commission (FTC).

The issue came from Google's breach of its privacy policy and involved explicitly misleading users of Apple's Safari web browser about privacy safeguards. The FTC held Google accountable for installing tracking cookies for advertising without users' knowledge or consent in the Safari web browser. While providing targeted advertisements, Google committed this breach. The FTC found that Google's activities were against an earlier administrative ruling imposed in the 2011 case of *FTC v. Google Inc.*[61]

Similar to this, the United States Department of Justice (DOJ) filed a federal antitrust lawsuit against Google LLC on October 20, 2020.[62] According to the lawsuit, Google engaged in anti-competitive behaviour in the markets for search engines and search advertising, in violation of the Sherman Antitrust Act of 1890. However, Judge Amit Mehta has tentatively slated September 12, 2023, as the beginning of the trial in the Justice Department's antitrust action against Google.[63]

Similarly, in a decision issued on June 2017, the European Commission (EC) found that Google had violated Article 102 of the Treaty on the Functioning of the European Union (TFEU) by misusing its dominant position on the market for general online search services to favour its own comparison-shopping service over rival comparison-shopping services.

Google was hit with a record-breaking 2.4 billion euros in penalties by the European Commission. Google disputed the allegations. However, Google's appeal of the

[60] United States v. Google, Inc., 3:12-cv-04177, (N.D. Cal. Nov, 16 2012).
[61] In the Matter of Google Inc., FTC File No. 102 3136 (complaint filed Mar. 30, 2011) <https://www.ftc.gov/legal-library/browse/cases-proceedings/102-3136-google-inc-matter> accessed 30 June 2023.
[62] United States and Plaintiff States v. Google LLC, No. 1:20-cv-03010, (D.D.C. Oct. 20, 2020).
[63] Lauren Feiner, 'DOJ case against Google likely won't go to trial until late 2023, judge says.' (CNBC, 18 December 2020) <https://www.cnbc.com/2020/12/18/doj-case-against-google-likely-wont-go-to-trial-until-late-2023-judge-says.html> accessed 30 June 2023.

Commission's decision that it had abused its dominant position was primarily rejected by the General Court.[64]

In another similar case, the European General Court in Luxembourg concluded that, to increase the dominance of its search engine, Google improperly imposed restrictions on mobile network providers and manufacturers of Android devices. The court upheld the Commission's verdict to fine Google €4.125 billion based on the gravity and length of the breach.[65]

The "right to be forgotten" was created in a historic ruling by the Court of Justice of the European Union (CJEU), which said that people had the right to ask search engines like Google to erase links to personal information that is incorrect, insufficient, irrelevant, or excessive.[66] Mario Costeja González, a Spanish national, brought the action by asking Google to take down links to a newspaper article regarding his previous debts, claiming that the search results violated his right to privacy. The decision had a big impact on privacy and data protection, and it changed how Europe's digital environment looked.

According to the CJEU, search engines are considered data controllers, and users have the right to ask that search results with excessive, irrelevant, or erroneous personal information be removed. The General Data Protection Regulation (GDPR) was adopted because of this ruling, which emphasised the value of privacy and data protection and shaped what was expected of search engines and online platforms.[67]

3.3.2. AMAZON.COM, INC.

Jeff Bezos established Amazon Inc. in 1994, and it has since grown into a major player in the e-commerce sector, especially in the digital economy. Amazon began as a digital bookstore, but it rapidly grew to include a variety of consumer items and eventually a worldwide marketplace. Its position as a top choice for millions of users throughout the world has been cemented by its user-friendly interface, effective

[64] Google and Alphabet v. Commission (Google Shopping) (T-612/17) ECLI:EU:T:2021:763 (10 November 2021).
[65] Google and Alphabet v. Commission (Google Android) (T-604/18) ECLI:EU:T:2022:541 (14 September 2022).
[66] Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González (C-131/12) ECLI:EU:C:2014:317 (13 May 2014).
[67] Google Spain SL, Google Inc. V Agencia Española de Protección de Datos (AEPD) and Mario Costeja González (C-131/12) ECLI:EU:C:2014:317 (13 May 2014).

delivery services, and affordable pricing. Amazon has a substantial market position, as evidenced by the fact that its net sales in 2022 topped $514 billion.[68]

The variety and innovations of Amazon have contributed to its success. One of its noteworthy projects is Amazon Web Services (AWS), a renowned cloud computing platform introduced in 2006.[69] Numerous businesses throughout the world are drawn to AWS because of its extensive package of services, which includes processing power, storage, and databases. The profitability of Amazon has greatly benefited from this diversification.

Amazon has made great progress in the digital content and entertainment industries with its Amazon Prime membership programme, which offers advantages including fast delivery, streaming services, and discounts. While Netflix and Disney+ are competitors for Amazon's streaming service, Prime Video, the company has substantially invested in original content creation to bolster its position. The voice-activated virtual assistant Alexa, which is powered by Artificial Intelligence (A.I) and gives consumers voice control over smart home appliances, information access, and music playback, is what propels the company's technical achievements.

Amazon's AI capabilities improve recommendation systems, inventory control, and shipping, enhancing the entire customer experience. Additionally, quick and dependable delivery is ensured by the company's efficient supply chain management and logistics, which are supported by a vast worldwide network of fulfilment centres and distribution hubs. To further speed up service to consumers, Amazon is investigating cutting-edge delivery techniques, including drones and autonomous automobiles.[70]

Amazon's Ring doorbell and home security system came under fire for sharing video footage with law enforcement agencies as part of its collaboration with them. Concerns focused on possible invasions of privacy and widespread surveillance. Critics contend that the collaborations lack transparency and accountability, threaten civil freedoms, and blur the boundaries between public and private settings.

---

[68] Statista Research Department, 'Annual net sales revenue of Amazon from 2004 to 2022.' (*Statista*, 14 February 2023) <https://www.statista.com/statistics/266282/annual-net-reenue-of-amazoncom/> accessed 30 June 2023.

[69] Amazon Web Services (AWS), 'Cloud computing with AWS.' <https://aws.amazon.com/what-is-aws/> accessed 30 June 2023.

[70] Amazon, 'About Amazon' <https://www.aboutamazon.com/> accessed 30 June 2023.

Amazon has added privacy protections and rules, but debate persists. To guarantee that these collaborations strike a balance between public safety and individual privacy rights, the debates emphasise the necessity for explicit legislation, supervision, and public education.[71]

Amazon Web Services (AWS) created Amazon Rekognition, a facial recognition system. Although it could be beneficial, there are issues with how law enforcement organisations employ it. As Rekognition permits real-time tracking and identification of people from numerous sources, mass surveillance is a major cause for concern. As a result, private rights may be violated by an all-encompassing monitoring state.

Additionally, racial and gender biases in facial recognition algorithms raise serious concerns. It can support prejudice and worsen inequality if it exists in rekognition. Rekognition deployments without protections, such as giving technology to law enforcement organisations, have sparked concerns about abuse and civil rights abuses. Civil rights organisations, academics, and even Amazon workers have all called for regulation, transparency, and ethical usage.[72]

The EU General Data Protection Regulation was allegedly infringed by Amazon Europe Core S.à r.l.'s processing of personal data, according to a judgement against Amazon made on July 16, 2021, by the Luxembourg National Commission for Data Protection (the "CNPD")[73]. A €746 million fine and accompanying practise changes are mandated by the ruling. The equivalent penalty under European data privacy legislation would be $887 million US, making it the largest penalty ever. Amazon did not outline the new business practises the commission is recommending, and the CNPD did not publicly disclose its judgement.[74]

3.3.3. APPLE INC.

[71] Diane Bartz, 'Amazon's Ring used to spy on customers, FTC says in privacy settlement.' (*Reuters*, 30 June 2023) <https://www.reuters.com/legal/us-ftc-sues-amazoncoms-ring-2023-05-31/> accessed 30 June 2023.

[72] Brian Barrett, 'Lawmakers can't ignore facial recognition's bias anymore.' (*Wired*, 26 July 2018) <https://www.wired.com/story/amazon-facial-recognition-congress-bias-law-enforcement/> accessed 30 June 2023.

[73] National Commission for Data Protection Luxembourg, 'Decision regarding Amazon Europe Core S.à r.l.' (06 August 2021) <https://cnpd.public.lu/en/actualites/international/2021/08/decision-amazon-2.html> accessed 30 June 2023.

[74] Reuters, 'Amazon hit with record EU data privacy fine.' (*Reuters*, 30 July 2021) <https://www.reuters.com/business/retail-consumer/amazon-hit-with-886-million-eu-data-privacy-fine-2021-07-30/> accessed 30 June 2023.

With products like the iconic iPhone, Mac computers, and Apple Watch, Apple Inc. is a well-known technological company on a global scale. Apple was founded in 1976 by Steve Jobs, Steve Wozniak, and Ronald Wayne.[75] With its cutting-edge designs, approachable user interfaces, and seamless hardware and software integration, Apple has revolutionised the IT sector. With a focus on simplicity, usability, and beauty, Apple has amassed a passionate following of customers throughout the world.

The corporation's constant dedication to quality, ground-breaking technological developments, and visionary leadership that continually pushes the envelope are all responsible for its success. Due to its dominance in the industry and devoted following of customers, Apple has continuously been listed among the most valuable brands in the world.[76] Apple's massive influence continues to redefine how the digital economy operates.

On August 31, 2014, the unauthorised release, circulation, and publication of 500 or more celebrity private photos, most of which belonged to women, took place.[77] This scandal was termed 'Fappening' or 'Celebgate'. Following their first posting on 4chan, these pornographic photographs swiftly gained popularity on sites like Reddit and Imgur.

Apple Inc. later emphasised that targeted spear phishing attempts were to blame, contrary to earlier speculation that the breach was caused by a vulnerability in their iCloud API. The attackers targeted certain people with misleading emails, coercing them into disclosing their login information, which gave them access to their iCloud accounts and the stolen images. The event highlighted the necessity for strict security procedures and knowledge of phishing efforts and generated concerns about digital privacy, security, and the moral ramifications of distributing stolen private content.

A research study by Lockdown and The Washington Post found that some iPhone apps are still collecting and transmitting user data, despite Apple's implementation of the 'App Tracking Transparenc' (ATT) feature, which attempts to give users greater

[75] United States Securities and Exchange Commission, 'Apple Inc. Fiscal 2022 Annual Report (Form 10-K)' (28 October 2022) <https://www.sec.gov/ix?doc=/Archives/edgar/data/320193/000032019322000108/aapl-20220924.htm> accessed 30 June 2023.
[76] Statista Research Department, 'Apple's global brand value from 2006 to 2022.' (*Statista*, 03 April 2023) <https://www.statista.com/statistics/326052/apple-brand-value/> accessed 30 June 2023.
[77] Dan Kedmey, 'Hackers Leak Explicit Photos of More Than 100 Celebrities' (*Time*, 01 September 2014) <https://time.com/3246562/hackers-jennifer-lawrence-cloud-data/> accessed 30 June 2023.

ownership over their privacy by permitting them to choose whether apps can track their activity for targeted advertising.[78]

The study examined 10 well-known iPhone applications on both iOS 14.8 and the recently released iOS 15 and discovered that several apps continued to gather and send user data even when users chose the "Ask app not to track" option.

The possibility that certain applications may circumvent Apple's privacy feature, thus compromising users' control over their data, is raised by this disclosure. It implies that there could be flaws or non-compliance from some app developers despite Apple's attempts to improve privacy protection.

It's crucial to remember that the success of the ATT feature hinges on app developers adhering to Apple's rules. Apple provides the structure for privacy protection, but it is up to developers to make sure their apps honour user preferences and privacy settings.

This incident illustrates how difficult it is to maintain user privacy in the digital era. Apple's ATT feature empowers consumers, but it also emphasises the necessity for ongoing watchfulness. To keep control over their personal information, individuals should scrutinise the data practises of the applications they use, and Apple must successfully enforce its standards.

The Federal Bureau of Investigation (FBI) and Apple Inc. have engaged in several court disputes over the unlocking of encrypted iPhones to assist in criminal investigations. These disputes are referred to as the "FBI-Apple encryption dispute." The conflict started in 2015 and 2016 and spurred a larger discussion about how to balance privacy and national security.

The FBI repeatedly requested court orders under the All Writs Act[79] to unlock iPhones that were part of criminal investigations. According to the Supreme Court, the All Writs Act (AWA) enables courts to issue writs to parties in order to support jurisdiction and preserve legal principles by taking into account elements such as their involvement, burden, and necessity.[80]

---

[78] Geoffrey A. Fowler and Tatum Hunter, 'When you "Ask app not to track", some iPhone apps keep snooping anyway'. (*The Washington Post*, 23 September 2021) <https://www.washingtonpost.com/technology/2021/09/23/iphone-tracking/> accessed 30 June 2023

[79] 28 U.S.C. § 1651.

[80] United States v. New York Telephone Co., 434 U.S. 159 (1977).

The orders mostly targeted iPhones with earlier operating systems that Apple was able to unlock, but they also included requests for help with more secure handsets that needed Apple to develop new software.

In 2016, the United States District Court for the Central District of California heard the most noteworthy case.[81] To unlock an iPhone 5C used by one of the gunmen in the massacre in San Bernardino, California, in December 2015, the FBI turned to Apple Inc. for assistance. Apple refused to develop the FBI's requested software, citing concerns over the potential impact on user privacy and encryption security.

A court hearing was planned, but the FBI was able to prolong it by claiming to have discovered a third party who could unlock the iPhone. The FBI then dropped its request after announcing that it had successfully unlocked the iPhone.[82] It was eventually discovered that the iPhone didn't contain any crucial information about the attack.[83]

In another Brooklyn case, a magistrate court decided that the All Writs Act could not be invoked to persuade Apple to unlock an iPhone. After acquiring the right passcode, the government appealed the decision but ultimately decided to dismiss the case.[84]

Such incidents sparked a wider debate on how to strike a compromise between the right to privacy of individuals and the requirement for law enforcement to have access to encrypted digital products and services.[85]

Building backdoors or weakening encryption, according to critics, might have significant effects on security and privacy since it could expose user data to hackers and repressive governments. Access to encrypted data, according to those who

[81] In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203, No. ED 15-0451M (C.D. Cal. Feb. 16, 2016).
[82] Danny Yadron, 'FBI confirms it won't tell Apple how it hacked San Bernardino shooter's iPhone' (*The Guardian*, 28 April 2016) <https://www.theguardian.com/technology/2016/apr/27/fbi-apple-iphone-secret-hack-san-bernardino> accessed 30 June 2023.
[83] Joseph Tanfani, 'Race to unlock San Bernardino shooter's iPhone was delayed by poor FBI communication, report finds' (*Los Angeles Times*, 27 March 2018) <https://www.latimes.com/politics/la-na-pol-fbi-iphone-san-bernardino-20180327-story.html> accessed 30 June 2023.
[84] Julia Harte, Julia Edwards and Julia Love, 'N.Y. judge backs Apple in encryption fight with government' (*Reuters*, 01 March 2016) <https://www.reuters.com/article/us-apple-encryption-deny-idUSKCN0W22Q0> accessed 30 June 2023.
[85] Mark Skelton, 'What the Apple versus FBI Debacle Taught Us' (*Scientific American*, 20 May 2016) <https://blogs.scientificamerican.com/guest-blog/what-the-apple-versus-fbi-debacle-taught-us/> accessed 30 June 2023.

supported the government's stance, is crucial for detecting and stopping illegal activity, especially when it pertains to matters of national security.

3.3.4. META INC.

Multinational technology corporation Meta Inc., formerly known as Facebook Inc., focuses on social networking, technological platforms, and digital services. Along with his undergraduate roommates Eduardo Saverin, Andrew McCollum, Dustin Moskovitz, and Chris Hughes, Mark Zuckerberg established it in February 2004.[86]

The main offering from Meta is the social networking site 'Facebook', which links billions of users globally and makes it possible for individuals to share material, interact, and establish connections with friends, family, and organisations. The corporation currently offers several additional well-known digital platforms and services, although its offerings have grown over time.

Significant acquisitions and advancements in a variety of technological fields have been accomplished by Meta Inc. 'Instagram', a well-known social networking service for sharing photos and videos, was purchased by Meta in 2012.[87] Instagram continues to run as a distinct platform under the Meta umbrella despite the acquisition and has grown significantly while under Meta's management.

Another significant acquisition by Meta in 2014 was the purchase of 'WhatsApp', a cross-platform messaging and voice over IP (VoIP) service.[88] Like Instagram, WhatsApp runs autonomously but gains access to Meta's substantial infrastructure and resources.

Furthermore, Meta widened its virtual reality sphere of influence by purchasing 'Oculus VR' in 2014.[89] The Oculus Rift headgear is a trademark of the renowned virtual reality technology firm Oculus VR. Meta has been actively involved in the development of virtual reality technology and applications via the Meta Reality Labs division.

---

[86] Meta Inc, 'Company information, Culture and Principles - About Meta' <https://about.meta.com/company-info/> accessed 30 June 2023.

[87] Meta Newsroom, 'Facebook to Acquire Instagram' (09 April 2012) <https://about.fb.com/news/2012/04/facebook-to-acquire-instagram/> accessed 30 June 2023.

[88] Meta Newsroom, 'Facebook to Acquire WhatsApp' (February 19, 2014) <https://about.fb.com/news/2014/02/facebook-to-acquire-whatsapp/> accessed 30 June 2023.

[89] Meta Newsroom, 'Facebook to Acquire Oculus' (March 25, 2014) <https://about.fb.com/news/2014/03/facebook-to-acquire-oculus/> accessed 30 June 2023.

‘Workplace’ by Facebook, a tool for corporate communication and collaboration released by Meta in 2016, is intended to improve productivity and communication inside organisations. Businesses now have an exclusive space for internal communication and cooperation thanks to this platform.

Meta has made substantial investments in AI research and development because of its understanding of the significance of artificial intelligence (AI). The corporation uses artificial intelligence (AI) technology to support several platform functions, including content suggestions and improvements to user experiences.

Facebook has come under criticism for purportedly assisting the government's surveillance of people. For instance, Edward Snowden’s revelations in 2013 disclosed that the U.S. National Security Agency (NSA) had gained access to user information from several technology companies, including Facebook.[90] Concerns were expressed over the scope of surveillance by the government and the participation of various social networking sites.

The “Cambridge Analytica” scandal, which involved the exploitation of private data from millions of Facebook users, was an issue of concern that broke out in 2018.[91] The British consulting company Cambridge Analytica specialised in data analysis and strategic communication. For political parties and organisations, the company allegedly offers analytics and behavioural targeting.[92] It was established in 2013 as a subsidiary of the SCL Group, a company that specialises in defence and strategic communication.

Aleksandr Kogan, a researcher from the University of Cambridge, and Cambridge Analytica worked together in 2014 to gather Facebook user data for academic research.[93] Kogan created the app “This Is Your Digital Life,” which provided

[90] Shirin Ghaffary, ‘Edward Snowden says Facebook is just as untrustworthy as the NSA’ (*Vox*, 31 October 2019) <https://www.vox.com/recode/2019/10/31/20940532/edward-snowden-facebook-nsa-whistleblower> accessed 30 June 2023.
[91] Nicholas Confessore, ‘Cambridge Analytica and Facebook: The Scandal and the Fallout So Far’ (*The New York Times*, 04 April 2018) <https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html> accessed 30 June 2023.
[92] ibid.
[93] Julia Carrie Wong, Paul Lewis and Harry Davies, ‘How academic at centre of Facebook scandal tried and failed to spin personal data into gold’ (*The Guardian*, 24 April 2018) <https://www.theguardian.com/news/2018/apr/24/aleksandr-kogan-cambridge-analytica-facebook-data-business-ventures> accessed 30 June 2023.

Facebook users with personality tests and psychological evaluations.[94] The programme not only gathered information from users who installed it but also from users' friends, allowing the unintentional acquisition of data from tens of millions of people.

In contravention of Facebook's regulations, Cambridge Analytica and Kogan exchanged the information with each other, allowing Cambridge Analytica to create comprehensive psychological profiles of individuals.[95] The 2016 US presidential election and the UK's Brexit vote both reportedly involved the use of these profiles for targeted political campaigning and influence activities.[96]

Through investigations by The Guardian and The New York Times, the Cambridge Analytica controversy was made public in March 2018.[97] In addition to raising questions about Facebook's privacy policies and the possibility of the manipulation of political processes, the articles showed the scope of data exploitation.

The controversy had serious consequences. Increased regulation of social media corporations was demanded as a result of the public outrage it produced and the numerous investigations that followed. Facebook came under fire for its insufficient privacy protection procedures, how it handled user information, and its involvement in the incident.

Several investigations were started because of the controversy.[98] The Federal Trade Commission (FTC) in the United States initiated an investigation, and consequently, Facebook was fined $5 billion for infringing the terms of a 2012 consent agreement.[99] The settlement, one of the biggest fines ever levied by the United States government for a violation, was accepted by a 3-2 vote.[100]

---

[94] ibid.
[95] Hilary Osborne and Hannah Jane Parkinson, 'Cambridge Analytica scandal: the biggest revelations so far' (*The Guardian*, 22 March 2018) <https://www.theguardian.com/uk-news/2018/mar/22/cambridge-analytica-scandal-the-biggest-revelations-so-far> accessed 30 June 2023.
[96] ibid.
[97] Carole Cadwalladr and Emma Graham-Harrison, 'Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach' (*The Guardian*, 17 March 2018) <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>
[98] Cristina Criddle, 'Facebook sued over Cambridge Analytica data scandal' (BBC, 28 October 2020) <https://www.bbc.com/news/technology-54722362> accessed 30 June 2023.
[99] United States v. Facebook, Inc., 1:19-cv-02184, (D.D.C.)
[100] Julia Carrie Wong, 'Facebook to be fined $5bn for Cambridge Analytica privacy violations – reports' (*The Guardian*, 12 July 2019)

In addition, Facebook agreed to pay the U.S. Securities and Exchange Commission (SEC) $100 million as part of a settlement in the same month for misleading investors about the potential risks of the exploitation of user data.[101] Despite learning of the data misuse in 2015, the SEC alleged that Facebook did not update its disclosure, leaving it unaltered for more than two years.

Additionally, looking into Cambridge Analytica, the United Kingdom Information Commissioner's Office (ICO) penalised Facebook £500,000 for failing to secure user data.[102] The controversy sparked more awareness and conversations about data privacy and protection, and it influenced the development of data protection laws like the General Data Protection Regulation (GDPR) of the European Union.

Following the investigation into Cambridge Analytica, various media outlets emphasised the systemic risk to human rights presented by Facebook's extensive surveillance of billions of users.[103] The reports emphasised the pressing requirement for a thorough overhaul of the corporation's primary operating strategy.

According to several articles, Facebook's vast data collection and surveillance techniques have significant ramifications regarding individual privacy and freedom of speech.[104] Their demand for reform illustrated the need to address the inherent dangers and negative effects linked to the pervasive surveillance of individuals by large technological corporations.

Recently, following an investigation into its data transfer practises, Meta Platforms Ireland Limited (Meta IE), the corporation that runs Facebook, received a record-

---

<https://www.theguardian.com/technology/2019/jul/12/facebook-fine-ftc-privacy-violations> accessed 30 June 2023.

[101] SEC v. Facebook, Inc. Case No. 3:19-cv-04241-JD (N.D. Cal)

[102] Reuters Staff, 'Facebook agrees to pay UK fine over Cambridge Analytica scandal' (*Reuters*, 30 October 2019) <https://www.reuters.com/article/us-facebook-privacy-britain-idCAKBN1X913O> accessed 30 June 2023.

[103] Amnesty Press Release, 'Facebook and Google's pervasive surveillance poses an unprecedented danger to human rights' (*Amnesty International*, 21 November 2019) <https://www.amnesty.org/en/latest/press-release/2019/11/google-facebook-surveillance-privacy/> accessed 30 June 2023.

[104] Amnesty Press Release, 'Facebook and Google's pervasive surveillance poses an unprecedented danger to human rights' (Amnesty International, 21 November 2019) <https://www.amnesty.org/en/latest/press-release/2019/11/google-facebook-surveillance-privacy/> accessed 30 June 2023.

breaking penalty of 1.2 billion euros from the Irish Data Protection Authority (IE DPA).[105]

The IE DPA was directed to enforce the penalties by the European Data Protection Board (EDPB), which issued a binding dispute settlement ruling.[106] This fine results from Meta IE's use of standard contractual clauses (SCCs), which the authorities judged to be in violation of the General Data Protection Regulation (GDPR), to transmit personal data to the United States since July 2020.

In accordance with the ruling, Meta IE must comply with the GDPR for all data transfers. Taking into mind the seriousness of the infraction, the EDPB established a starting point for computing the fine between 20% and 100% of the maximum permitted amount. Additionally, Meta IE must stop processing and storing personal data of European users illegally in the United States within six months of obtaining the IE DPA's final ruling.[107]

The final verdict of the IE DPA concurs with the EDPB's legal analysis. Following a dispute resolution process that was sparked by complaints voiced by several concerned supervisory authorities (CSAs), the EDPB made its determination based on Article 65(1)(a) of the GDPR.[108] The CSAs had protested to Meta IE and asked for an administrative penalty and an order for obedience to the laws governing data processing.

Given the massive amount of Facebook users in Europe and the systematic, repeated, and ongoing nature of the data transfers, the EDPB considered Meta IE's violation as highly significant. Overall, the penalty issued on Meta IE represents a significant enforcement action, emphasising the importance of GDPR compliance and possible repercussions for companies that fail to comply with the rules governing data protection.

3.3.5. MICROSOFT INC.

[105] European Data Protection Board (EDPB), '€1.2 billion fine for Facebook as a result of EDPB binding decision' (EDPB, 22 May 2023) <https://edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en> accessed 30 June 2023.
[106] Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems Case C-311/18, ECLI:EU:C:2020:559 (16 July 2020).
[107] European Data Protection Board (EDPB), '€1.2 billion fine for Facebook as a result of EDPB binding decision' (EDPB, 22 May 2023) <https://edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en> accessed 30 June 2023.
[108] ibid.

Microsoft Inc., a multinational technological corporation with its headquarters in Redmond, Washington, was established by Bill Gates and Paul Allen in 1975.[109] Microsoft has become one of the most notable corporations in the technology sector because of its long history and widespread presence, offering a variety of hardware, software, and cloud services. Microsoft has always been at the forefront of innovation, consistently reshaping the digital environment.

The corporation is best known for Windows, which has served as the industry standard operating system for personal computers for decades. Microsoft has also created a wide range of other well-known software programmes, including Microsoft Office, Xbox gaming consoles, and the Azure cloud computing platform.[110]

Microsoft has made significant investments in its Azure platform with a focus on cloud computing, providing a full range of cloud-based services encompassing infrastructure, platform, and software-as-a-service solutions.[111] Because of this, the corporation is now positioned to compete with other industry titans like Amazon Web Services and Google Cloud in the rapidly evolving cloud sector.

Microsoft's worldwide brand worth surpassed 611 billion dollars in 2022. Microsoft's brand worth increased by an estimated 49% over the prior year, solidifying its place among the most valuable brands globally.[112]

Data and systems used by Microsoft's users are presently at risk due to a number of security breaches and vulnerabilities. In 2010, a zero-day bug in Internet Explorer made it possible for hackers to infiltrate significant American businesses, including Adobe and Google.[113] As a result of the vulnerability, attackers were given administrator powers, which allowed them to take control of systems, view private data, and establish new user accounts.

---

[109] Microsoft, 'About us' <https://www.microsoft.com/en-us/about> accessed 30 June 2023.
[110] ibid.
[111] Microsoft Corporation, 'Microsoft Annual Report 2022.' (28 July 2022) <https://www.microsoft.com/investor/reports/ar22/ > accessed 30 June 2023.
[112] Statista Research Department, 'Microsoft's global brand value from 2006 to 2022.' (*Statista*, 06 January 2023) <https://www.statista.com/statistics/326058/microsoft-brand-value/> accessed 30 June 2023.
[113] Charles Arthur, 'Microsoft warns of new zero-day flaw targeting Internet Explorer' (*The Guardian*, 18 September 2012) <https://www.theguardian.com/technology/2012/sep/18/microsoft-internet-explorer-zero-day-flaw> accessed 30 June 2023.

In 2013, users' Xbox Live login information was made public after information from a survey and prize draw was inadvertently posted online.[114] Although it is yet unknown if prospective attackers were able to access the data, it prompted questions about user privacy and data protection.

In 2013, through a programme known as PRISM, the US National Security Agency (NSA) allegedly had direct access to the networks of significant US internet service corporations, including Microsoft, Google, Facebook, and Apple.[115] The NSA had the ability to gather many types of data via Prism, including search history, email content, file transfers, and live conversations, according to a top-secret document that was acquired by The Guardian. The software allowed for broad monitoring of both saved data and live conversations.

Since the programme's launch in 2007, it has been claimed that some of the biggest digital corporations in the world have gotten involved. One of the first was Microsoft, and the data gathering process started in December 2007.[116] Changes to US surveillance law made under President Bush and later renewed under President Obama in December 2012 made it possible for the NSA to have access.[117]

The National Security Agency (NSA) may have had direct access to Microsoft's servers due to the company's participation in the PRISM surveillance programme, which was made public in 2013.[118] According to papers leaked by Edward Snowden, the NSA obtained user information from Microsoft services including Outlook.com, Skype, and OneDrive.[119]

Microsoft and other involved corporations, on the other hand, denied offering uncontrolled access, claiming that they only gave information in response to

---

[114] Caroline Donnelly, 'Xbox Live users hit by data breach.' (*ITPRO*, 20 March 2013) <https://www.itpro.com/data-leakage/19470/xbox-live-users-hit-data-breach> accessed 30 June 2023.
[115] Glenn Greenwald and Ewen MacAskill, 'NSA Prism program taps in to user data of Apple, Google and others' (*The Guardian*, 07 June 2013) <https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data> accessed 30 June 2023.
[116] ibid.
[117] Glenn Greenwald and Ewen MacAskill, 'Obama orders US to draw up overseas target list for cyber-attacks' (*The Guardian*, 07 June 2013) <https://www.theguardian.com/world/2013/jun/07/obama-china-targets-cyber-overseas> accessed 30 June 2023.
[118] Glenn Greenwald, Ewen MacAskill, Laura Poitras, Spencer Ackerman and Dominic Rushe, 'Microsoft handed the NSA access to encrypted messages' (*The Guardian*, 12 July 2013) <https://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data> accessed 30 June 2023.
[119] The Guardian, 'The Snowden files' (*The Guardian*, 12 February 2017) <https://www.theguardian.com/world/series/the-snowden-files> accessed 30 June 2023.

legitimate government demands through accepted legal channels. Microsoft reaffirmed its dedication to customer privacy and emphasised the fact that it does not engage in broad data sharing. It's significant to highlight that the precise scope of Microsoft's involvement is still unknown, given the informational nature of the stolen papers.

On 30 June 2016, The Commission Nationale de l'Informatique et des Libertés (CNIL; English: National Commission on Informatics and Liberty), France's data protection administrative regulatory authority, had issued an order requiring Microsoft to stop storing excessive amounts of user data and to cease tracking Windows 10 users' internet browsing habits without their permission.[120]

The CNIL also directed Microsoft to take actions to protect the security and confidentiality of the private data of users since the corporation was still transferring data to the US in compliance with the "Safe Harbour" arrangement, which a European Union court had determined to be unlawful. Microsoft was given a three-month timeframe to abide by these instructions.[121]

The CNIL's conclusion was prompted by an investigation carried out between April and June in response to inquiries from European data protection authorities after the release of Windows 10.

The CNIL discovered that Microsoft had been gathering an enormous amount of user data, including app downloads and usage durations.[122] Additionally, it was discovered that Microsoft used cookies without providing enough notice or opt-out options to provide personalised ads.

The CNIL forewarned Microsoft that failure to comply might result in the appointment of an investigator and the recommendation of sanctions. The commission made it explicit that its goal is to protect individuals' freedom of choice and

[120] Reuters, 'France orders Microsoft to stop collecting excessive user data' (*Reuters*, 21 July 2016) <https://www.theguardian.com/technology/2016/jul/20/france-microsoft-user-data-collection-privacy> accessed 30 June 2016.
[121] Amar Toor, 'France orders Microsoft to stop tracking Windows 10 users' (*The Verge*, 21 July 2016) <https://www.theverge.com/2016/7/21/12246266/france-microsoft-privacy-windows-10-cnil> accessed 30 June 2023.
[122] Mark Coppock, 'France's National Data Protection Commission says Windows 10 collects too much data' (*onmsft.com*, 20 July 2016) <https://www.onmsft.com/news/frances-national-data-protection-commission-says-windows-10-collects-much-data/>

information, not to ban advertising. Similar warnings from CNIL have previously been sent to other US digital corporations, including Google and Facebook.

In 2013, there was an issuance of a warrant[123] requiring Microsoft to turn over emails and other data related to a customer account suspected of being used in the trafficking of illicit drugs. Because the account's data was kept in Microsoft's data centre in Dublin, Ireland, the corporation contested the request.[124]

Microsoft attempted to get the warrant revoked, but the court found them in civil contempt. The Second Circuit Court of Appeals overturned the ruling, claiming that applying the statute extraterritorially to enforce the warrant would be illegal.[125]

In March 2018, the Clarifying Lawful Overseas Use of Data (CLOUD) Act was approved by Congress in response to this case.[126] This legislation amended the Electronic Communications Privacy Act (ECPA) and updated the Stored Communications Act by declaring that service providers must adhere to the requirements to maintain, backup, or disclose electronic communication contents, records, or other information in their control, regardless of where it is located.

Later, after deciding that the matter was moot, the Supreme Court dismissed it.[127] The reason for this was that the original warrant had been replaced with a new one, and the parties had no active disagreements over the subject matter of the certiorari.

Significantly, this case brought up significant issues regarding the extraterritorial scope of US warrants and the rights to privacy enjoyed by individuals whose data is maintained abroad. The CLOUD Act's adoption defined service providers' responsibilities in certain circumstances and expanded US government access to digital communications and information held abroad.

In 2019, according to a report, without password security, almost 250 million Microsoft customers' private information was exposed online.[128] The data, which

[123] Issued under 18 U. S. C. §2703.
[124] In re Warrant to Search a Certain E-mail Account Controlled & Maintained by Microsoft Corp., 15 F. Supp. 3d 466, 470 (S.D.N.Y. 2014).
[125] Microsoft Corp. v. United States., 829 F.3d 197 (2d Cir. 2016)
[126] Consolidated Appropriations Act, 2018, Pub. L. No. 115-141 (March 23, 2018), Div V, CLOUD Act, amending the Electronic Communications Privacy Act, 18 U.S.C. 2701 et seq, <https://www.congress.gov/115/plaws/publ141/PLAW-115publ141.pdf>
[127] United States v. Microsoft Corp., 584 U.S. ___, 138 S. Ct. 1186 (2018)

encompasses a 14-year period from December 2005 to that same month in 2019, was found by Comparitech's security research team. They discovered five unprotected Elasticsearch servers with customer service and support logs that recorded communications between Microsoft support representatives and clients throughout the world.

The leaked data contained customer email addresses, IP addresses, geographic locations, descriptions of service and support claims, emails from Microsoft support agents, case numbers and outcomes, and private company notes, but much of the personally identifying material had been deleted.

Although at first glance this might not seem alarming, scammers operating Microsoft support scams might find it quite beneficial. The dataset's vulnerability was initially discovered on December 28, 2019, when the threat intelligence search engine BinaryEdge indexed them. Microsoft was alerted the next day by Bob Diachenko of Comparitech, and the business moved quickly to protect the servers within 24 hours.

This incident adds to a series of Microsoft-related breach of privacy issues,[129] which also include a crucial Windows 10 update notice about a significant cryptographic weakness and the absence of a fix for an actively exploited zero-day Internet Explorer vulnerability. The disclosure of client information highlights the need for strong security measures and serves as a warning of the possible dangers linked to insufficient data protection.

In summary, multinational corporations (MNCs) have an enormous impact on surveillance capitalism and digital colonialism, reshaping the world of technology and the digital economy in unprecedented ways. The dominance of large technology corporations based in the United States, like Google, Facebook, and Amazon, has allowed these corporations to use their technological prowess, financial capabilities, and market leadership to extract valuable user data and gain control over the digital economy. These companies have increased their global reach, influencing user behaviours, data collection practises, and market dynamics in many developing countries of the Global South.

---

[128] Davey Winder, 'Microsoft Security Shocker As 250 million Customer Records Exposed Online' (*Forbes*, 22 January 2020) <https://www.forbes.com/sites/daveywinder/2020/01/22/microsoft-security-shocker-as-250-million-customer-records-exposed-online/?sh=25f9bdb54d1b> accessed 30 June 2023.
[129] Michael X. Heiligenstein, 'Microsoft Data Breaches: Full Timeline Through 2023' (*Firewall Times*, 06 April 2023) <https://firewalltimes.com/microsoft-data-breach-timeline/> accessed 30 June 2023

Multinational corporations acquire a lot of data, frequently without the explicit permission of the user, to produce insightful profiles and data that may be offered to advertisers. The Cambridge Analytica incident involving Facebook is one noteworthy instance in which millions of users' personal information was obtained without their consent and used for political objectives. This lawsuit brought to light their unethical pursuit of private data for monetary gain.

In conclusion, there are many facets to the complex yet pervasive role that global corporations play in surveillance capitalism and digital colonialism. The provided examples and legal cases highlight the necessity for comprehensive and moral strategies to protect individual rights, advance fair competition, and resolve power disparities brought about by multinational corporations' hegemony in the digital sphere.

CHAPTER 4

ROLE OF GLOBAL SOUTH GOVERNMENTS AND POLICYMAKERS IN DIGITAL COLONIALISM AND SURVEILLANCE CAPITALISM

The emergence of the digital age has fundamentally changed how individuals and societies operate, interact, and communicate. A new concern has developed, meanwhile, amid the promises of connectedness and advancement: the part that governments and policymakers in the global South play in digital colonialism and surveillance capitalism. The phenomenon demonstrates the complex interrelationships between technology, power, and the digital exploitation of data.

Powerful multinational corporations with headquarters mostly in the global North currently control most of the digital platforms and infrastructure that affect the daily lives of individuals. These corporations have a lot of influence over how information is shared, data is gathered, and online interactions are created. Governments and policymakers in the Global South frequently find themselves stuck between the demand to adhere to the norms established by these influential entities and their ambitions for economic advancement, along with respect for privacy and the protection of individuals private information.

The countries of the Global South are lucrative marketplaces for the growth of surveillance capitalism because of their massive populations and expanding digital environments. In the digital age, establishing policies and procedures to protect personal information and ensure privacy is vital. However, the intricate relationships between authority and influence frequently result in compromises that put monetary benefits ahead of the rights and freedoms of an individual.

A thorough examination of the social, economic, and political environments in which global South governments and policymakers' function is necessary to comprehend their involvement in digital colonialism and surveillance capitalism. The difficulties faced by policymakers in these regions are a result of historical legacies of colonisation, economic dependence, and power asymmetries between global North and global South entities.

By exploring how lawmakers and policymakers have shaped the digital realm, this chapter seeks to analyse the complex aspects of digital colonialism and surveillance capitalism in the global South. We may learn more about the approaches used by governments in the global south to deal with the challenges of the digital era by examining legal frameworks and policy decisions. The ultimate objective is to highlight prospective possibilities for fair and inclusive digital advancement, ensuring that the developing countries of the Global South can actively contribute to crafting their digital future while defending the rights and interests of their citizens.

The term 'Global South,' which was first used in 1969 by progressive social activist Carl Oglesby, is a euphemism for phrases like 'developing countries,' 'least developed countries,' 'underdeveloped countries,' 'low-income economies,' and the out-of-favour 'third world countries.'[130]

The phrase 'Global South' is used to characterise countries with underdeveloped economies that struggle with issues including low per capita income, high unemployment, and a lack of valued capital.[131] The term refers to a collection of countries that are seen as less economically developed than those of the global north and are frequently located in the southern hemisphere.[132] It is a socioeconomic and political notion. The term 'Global South' refers to a wide range of geographical areas, including sections of Latin America, Africa, Asia, and the Caribbean.

Few socioeconomic words, however, are more hotly contested, potentially controversial, or commonly misunderstood. It's crucial to remember that different contexts and criteria may lead to different classifications of countries as belonging to the Global South.[133] The socioeconomic standing of nations can also shift over time, which means that the composition of the Global South may also alter from time to time.[134]

---

[130] World Population Review, 'Global South Countries: A Complete List.' (2023) <https://worldpopulationreview.com/country-rankings/global-south-countries> accessed 30 June 2023.
[131] Parsa Arbab, 'Global and Globalizing Cities from the Global South: Multiple Realities and Pathways to Form a New Order.' (2019) 18 (3) Perspectives on Global Development and Technology 327.
[132] Nahzeem Oluwafemi Mimiko, *Globalization: The Politics of Global Economic Relations and International Business* (Durham, North Carolina Academic Press, 2012).
[133] Jean-Philippe Therien, 'Beyond the North-South divide: The two tales of world poverty.' (1999) 20 (4) Third World Quarterly 723.
[134] ibid.

There are numerous different laws and regulations that govern the use of data, internet and digital technologies in the countries of the Global South. The legislative frameworks, rules, and regulations in place in various countries of the Global South to handle data protection and privacy concerns are extensively examined in the sections that follow.

4.1. LEGAL AND REGULATORY FRAMEWORK IN INDIA

India is a key player in data privacy, especially regarding the idea of digital colonialism and surveillance capitalism. India is the most populous country in the world and a pioneer in information technology, thus its perspectives on data privacy and surveillance have a big impact on the world stage.

The Information Technology (IT) Act of 2000, the 2008 amendment to the Act, its subordinate legislations, which includes the Intermediary Guidelines Rules 2011, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, and the Personal Data Protection Bill, which is presently awaiting legislative approval[135], serve as the primary legal frameworks for data privacy in India. These legal frameworks strive to protect the private information of Indian citizens and provide standards for the administration, processing, and archiving of data. To guarantee that individuals' personal data is secured and not exploited, the proposed Personal Data Protection Bill combines concepts including data localization, consent, and responsibility.

The Information Technology (IT) Act of 2000 and its 2008 amendment are important pieces of legislation that protect against the surveillance of data while preserving individuals' rights to their personal information. The Act contains many provisions that apply to this scenario. Corporate entities managing sensitive personal information are required to employ appropriate security measures to safeguard it.[136]

Inaction might make the entity accountable for compensating the impacted parties for damages. To ensure that personal data is safeguarded from breaches and unauthorised use, the Act makes computer damage, data theft, and unauthorised access punishable

[135] PRS Legislative Research, 'Bill track: Draft Digital Personal Data Protection Bill 2022.' (*PRS INDIA*, June 2023) <https://prsindia.org/billtrack/draft-the-digital-personal-data-protection-bill-2022> accessed 30 June 2023.
[136] The Information Technology Act 2000, s 43A.

offences.[137] To avoid arbitrary surveillance, the Act establishes procedural controls on the government's ability to intercept, monitor, or decode computer-generated information.[138] Providing individuals with ownership of their data and avoiding unauthorised disclosure or misuse, it forbids the dissemination of private information without consent.[139]

Finally, the Act safeguards intermediaries, such as internet service providers and social media sites, from legal responsibility for third-party data held on those sites.[140] It does, however, place a duty on intermediaries to swiftly delete or prevent access to illegal content. Combined, these sections create a regulatory structure that ensures data privacy, establishes the duties and liabilities of different parties engaged in data processing and storage, and defends against unauthorised access and disclosure.

Digital surveillance in India is a complicated and evolving issue. On the one hand, the nation has experienced security concerns and fears about terrorism and digital threats, which have led to the deployment of surveillance mechanisms for the sake of national security. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021[141], for example, mandate that social media platforms and intermediaries abide by certain data disclosure and monitoring duties.

The Rules of 2021[142], replaced the previous Rules from 2011 and includes certain new standards for intermediaries, significant social media intermediaries (SSMIs), and digital media publishers. Intermediaries were immune from responsibility for third-party information under the 2011 Rules if they followed the rules for doing due diligence.

The 2021 Rules keep the 2011 Rules' due diligence requirements, such as defining categories of prohibited content, promptly removing content in response to court or government orders, assisting law enforcement, keeping track of blocked content and records, and implementing a grievance redressal mechanism.

[137] The Information Technology Act 2000, s 66.
[138] The Information Technology Act 2000, s 69.
[139] The Information Technology Act 2000, s 72A.
[140] The Information Technology Act 2000, s 79.
[141] Notification dated, the 25th February, 2021 G.S.R. 139(E): The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.
[142] ibid.

Rule 3(2), which requires intermediaries and social media platforms to have a user verification procedure, is an important rule. This helps to ensure accurate user data and stops the spread of fraudulent or deceptive content. Users can report privacy issues and content that is objectionable by using the grievance officer that intermediaries are required by Rule 4(1) to designate. Rule 4(2) encourages transparency and gives individuals the ability to know how their data is used by making privacy terms and conditions of use accessible.

However, India has also seen discussions and reservations about the possible violation of individual privacy rights brought on by surveillance practises. Aadhaar, a biometric identification system, has sparked concerns about surveillance and privacy.[143] While Aadhaar has made it possible to offer services effectively and implement social programmes that are specifically targeted, questions have been raised about how sensitive personal data is collected and stored.

The Indian Supreme Court ruled that Aadhaar's mandatory use violates privacy.[144] The court has recognised privacy as a basic right under the Indian Constitution, with reasonable restrictions. The court stressed the need for strict data protection legislation and suggested a comprehensive system to secure personal data. The decision establishes a precedent for protecting personal data and limiting government access to it in India.

India's participation in the realm of data colonialism is multifaceted. On the one hand, Indian companies and new start-ups are producing large volumes of data at an increasing rate, creating a chance for innovation and economic growth. However, there are worries that this information might be collected and processed by global corporations, turning Indian consumers into data subjects without having any authority or ownership over their own personal data.

Data localization, the requirement that data generated in India be stored and processed within the country, has been the subject of discussion. Arguments have been made both in favour of safeguarding national interests and guaranteeing data sovereignty and in opposition to concerns about obstructing international data flows and innovation.

[143] Pawan Singh, 'Aadhaar and data privacy: biometric identification and anxieties of recognition in India.' (2019) 24 (3) Information, Communication & Society.
[144] Justice K.S. Puttaswamy (Retd) Vs Union of India (2017) 10 SCC 1

The National Digital Health Mission and the National Payments Corporation of India's Unified Payments Interface (UPI), which seek to use data for the benefit of Indian citizens and lessen reliance on international technology corporations[145], are two examples of local data-driven initiatives that India has supported to combat data colonialism.

In 2016, a legal case was initiated by Karmanya Singh and Shreya Sethi against WhatsApp, pertaining to a matter concerning privacy and safeguarding of data. According to the petitioners, WhatsApp's 2016 privacy policy changes were meant to collect an extensive amount of user data for various purposes, which could infringe on users' private rights. The litigation was originally instituted in the Delhi High Court but was subsequently elevated to the apex court of India.[146]

The petition cited concerns over WhatsApp's privacy policy, user authorization, and Facebook's information alternatives. The petitioners said WhatsApp's policy changes violated the basic right to privacy enshrined in the Indian Constitution. WhatsApp stated its commitment to privacy, end-to-end encryption, and data security. Their response said user messages were not stored on their systems and end-to-end encryption prevented third-party access. The service provider provided alternatives to deleting accounts and data.

The court ordered Facebook to remove non-existent member data and limit access to member data on Facebook. It also called for a regulatory structure to be established. The court requested information disclosure policies from WhatsApp, Twitter, and Google. This case underlines the importance of data security and privacy rights in the digital age. The Supreme Court's ruling changed how individuals see rights pertaining to data privacy and led to comprehensive changes in data protection laws in India, affecting data security and privacy in the country.

On July 18, 2021, the Pegasus Project, a group of 17 media outlets and Amnesty International, revealed a list of 50,000 phone numbers that may have been affected by Pegasus spyware. Journalists, activists, and politicians affected by the Indian government's use of spyware petitioned for a judicial probe.

---

[145] India Brand Equity Foundation, 'Digital Payments and their impact on the Indian Economy.' (*IBEF.org*, April 2022) <https://www.ibef.org/research/case-study/digital-payments-and-their-impact-on-the-indian-economy> accessed 30 June 2023.

[146] Karmanya Singh Sareen & Anr. v. Union of India & Ors. (2019) 17 SCC 689

On October 27, the Court created a technical committee to investigate Pegasus in an interim order.[147] The court stressed that any acceptable privacy invasion must be proportional to the law's objective. National security does not exempt the Union government from accountability. The judiciary noted that an intrusion on privacy may impede an individual's freedom of speech. Surveillance is linked to press freedom, which is essential to democratic administration.

The bench appointed a technical committee under former Supreme Court Justice R.V. Raveendran. The committee investigates Pegasus's monitoring of Indian people and its legality. They must also advise on ways to improve the nation's cybersecurity standards to protect the public's right to privacy and develop grievance channels for unlawful surveillance.

The judicial committee must decide if the Indian government used Pegasus spyware on journalists, attorneys, and government officials. Upon determining whether the Union government has employed the Pegasus spyware, the Court will establish the parameters that the government must abide by when conducting surveillance on individuals.

In conclusion, India's position on data privacy considering digital colonialism and surveillance capitalism is nuanced. It includes striking a balance among issues of personal privacy, national security, and profitability from the digital economy.

India is working to preserve data privacy while addressing the difficulties presented by the digital era and international data flows, as seen by the changing regulatory landscape and continuing discussions.

4.2. LEGAL AND REGULATORY FRAMEWORK IN BRAZIL

Brazil has established comprehensive legal frameworks, policies, and regulations aimed at safeguarding personal data and upholding data privacy in the face of surveillance capitalism and digital colonialism. The General Personal Data Protection Law (LGPD) is the fundamental basis for data protection in Brazil and was implemented in September 2020[148].

[147] Manohar Lal Sharma v. Union of India, 2021 SCC OnLine SC 985

[148] Lei Geral de Proteção de Dados Pessoais (LGPD) Law No.13709/2018. <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm> accessed 30 June 2023.

The LGPD, which is patterned after the GDPR of the European Union, has a broad scope that encompasses both the public and private sectors. This includes foreign entities that handle the personal data of individuals who are residents of Brazil. The legal framework sets forth fundamental tenets governing the handling of data, encompassing lawfulness, purpose limitation, data minimization, accuracy, storage limitation, integrity, confidentiality, and accountability.

The significance of acquiring explicit, informed, and unequivocal consent from individuals for data processing endeavours is underscored by this. The LGPD confers several entitlements on individuals, including but not limited to access, rectification, erasure, and data portability, thereby empowering them to exercise authority over their personal data.

To adhere to the regulations set forth by the LGPD, entities that handle substantial quantities of personal data are required to designate a Data Protection Officer (DPO) who will be responsible for ensuring compliance with the provisions. In the event of a data breach, it is mandatory for data controllers to expeditiously inform both the impacted individuals and the National Data Protection Authority (ANPD), which functions as the principal regulatory entity.

The National Data Protection Authority (ANPD) was established by Brazil to enforce the LGPD and supervise data protection concerns.[149] The Brazilian National Data Protection Authority (ANPD) is tasked with the regulatory and supervisory oversight of data protection activities, as well as the promotion of awareness and the issuance of guidelines and recommendations to ensure compliance with the Brazilian General Data Protection Law (LGPD). The entity in question assumes a crucial function in overseeing and implementing measures related to safeguarding data privacy in Brazil.

Brazil's legal framework encompasses the Marco Civil da Internet, a comprehensive legislation that was implemented in 2014[150], in addition to the LGPD. Although its primary focus is not on data privacy, it incorporates clauses that are pertinent to safeguarding the data rights of individuals.

---

[149] Centre for Information Policy Leadership (CIPL) and Centro de Direito, Internet e Sociedade of Instituto Brasiliense de Direito Público (CEDIS-IDP), 'The Role of the Brazilian Data Protection Authority (ANPD) under Brazil's New Data Protection Law (LGPD)' (*CIPL-CEDIS-IDP Joint Project*, 17 April 2020)

[150] Marco Civil da Internet (Federal) Law No.12965/2014. <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm> accessed 30 June 2023.

The Marco Civil legislation maintains fundamental tenets such as the concept of net neutrality, which guarantees that internet service providers are prohibited from engaging in discriminatory practises or giving preferential treatment to content or applications. The statement acknowledges the significance of privacy and confidentiality as fundamental rights, thereby ensuring the protection of personal data and communication privacy.

Additionally, the Brazilian Internet Steering Committee (CGI.br), which develops and coordinates internet-related regulations, supports the preservation of data privacy[151]. While CGI.br does not have a specific focus on data privacy, it does facilitate public engagement in policy formation, enabling diverse stakeholders to participate in deliberations concerning data privacy, internet governance, and digital rights.[152]

The committee adheres to the fundamental values of openness, responsibility, unrestricted communication, and confidentiality in relation to the management of online activities, thereby making a valuable contribution to safeguarding personal information in Brazil.[153]

In 2016, A Sergipe state judge ordered Facebook Vice President for Latin America Diego Dzodan to be arrested and interrogated in Sao Paulo.[154] To protect an ongoing criminal investigation, WhatsApp, the Facebook-owned messaging service, did not reveal the specifics of the request.

The arrest was exceptional, but social media corporations usually follow local court judgements, especially in countries where they operate. Facebook deemed the arrest excessive. This occurred amid rising government requests for social media and internet corporations to help with surveillance and content filtering.

WhatsApp had minimal overseas operations before its acquisition by Facebook, making it less exposed to foreign government disputes. Due to Facebook's popularity,

---

[151] Brazilian Internet Steering Committee (CGI.br), 'About the CGI.br' (*CGI.br*, 30 June 1995) <https://www.cgi.br/about/#:~:text=The%20Brazilian%20Internet%20Steering%20Committee,well%20as%20promoting%20technical%20quality%2C> accessed 30 June 2023.

[152] Brazilian Internet Steering Committee (CGI.br), 'CGI.br publishes guidelines and recommendations for the application of Internet laws in Brazil' (*CGI.br Press Release*, 31 January 2018) <https://www.cgi.br/noticia/releases/cgi-br-publica-diretrizes-e-recomendacoes-para-aplicacao-de-leis-sobre-internet-no-brasil/> accessed 30 June 2023.

[153] ibid.

[154] Brad Haynes, 'Facebook executive jailed in Brazil as court seeks WhatsApp data' (*Reuters*, 01 March 2016) <https://www.reuters.com/article/us-facebook-brazil-idUSKCN0W34WF> accessed 30 June 2023.

governments may pressure the corporation by arresting executives. The presiding judge authorised an arrest after Facebook failed to comply with a 1 million reais (equivalent to $250,000) monetary penalty and failed to help investigators access WhatsApp communications in a drug trafficking case.

WhatsApp's 2014 adoption of end-to-end encryption makes monitoring messages across its network unlikely. WhatsApp's action, according to American Civil Liberties Union (ACLU) technologist Christopher Soghoian, is to distance itself from conducting surveillance efforts.

In 2018, the Brazilian Superior Court of Justice (STJ) issued an order to several search engines to eliminate links that connect a public prosecutor to fraud accusations, citing her 'right to be forgotten' as a basis for the decision.[155] DPN initiated legal action against Google, Yahoo!, and Microsoft with the aim of eliminating search results pertaining to her involvement in the 2006–2007 public tender for judgeships in the State of Rio de Janeiro.

The Court employed reasoning that prioritised the private interest of the individual over the public interest of information accessibility.[156] This was due to the extended period of over a decade that had passed since the relevant incidents.

The Court stated that the matter at hand does not pertain to the complete eradication of the past, but rather to the provision of a reasonable level of anonymity to the concerned individual to enable them to lead their life. The ruling by the STJ in Brazil was a significant milestone in the legal framework of the country, as it marked the very first case where de-indexation of search results has been permitted.

In conclusion, Brazil has established an extensive array of legal structures, policies, and regulations aimed at safeguarding personal data and upholding data privacy amidst the prevalence of surveillance capitalism and digital colonialism. The LGPD is the principal legal structure that highlights the significance of consent, individual rights, and accountability.

The Brazilian National Data Protection Authority (ANPD) is responsible for enforcing data protection regulations, while the Marco Civil da Internet and the

[155] DPN v. Google Brasil Internet Ltda (08 May 2018) Case No. 0218767-85.2009.8.19.0001.
[156] ibid.

Brazilian Internet Steering Committee (CGI.br) provide auxiliary support in ensuring the protection of data privacy.

The measures collectively establish a robust framework for safeguarding data in Brazil, endowing individuals with authority over their personal data and reducing the potential risks linked to surveillance capitalism and digital colonialism.

4.4. LEGAL AND REGULATIORY FRAMEWORK IN CHILE

In Chile, the protection of personal information and protecting data privacy in the context of surveillance capitalism and digital colonialism have emerged as major issues, leading to the construction of strong legal frameworks, rules, and regulations.

Chile was granted membership in the Organisation for Economic Co-operation and Development (OECD) in 2010,[157] thereby pledging to conform to data protection regulations and standardise cross-border data transmission. On 15 March 2017, the Chilean government introduced Bill No. 11144-07, which would regulate the processing and safeguarding of personal data and establish a Data Privacy Authority.[158]

The bill provides modifications to the existing law and ensures compliance with the standards set forth in the General Data Protection Regulation (Regulation (EU) 2016/679). Additionally, the bill requires the establishment of a dedicated agency responsible for overseeing data protection.

In 2018, the Chilean Constitution included data protection as a fundamental right.[159] Chile has aligned itself with other Latin American countries such as Colombia, Mexico, and Ecuador in incorporating provisions in their respective constitutions that safeguard the right to personal data protection.

---

[157] The Organization for Economic Cooperation and Development (OECD), 'Agreement on the terms of accession of the Republic of Chile to the Convention on the Organisation for Economic Co-operation and Development.' (*OECD.org*, 11 January 2010) <https://www.oecd.org/chile/44381035.pdf> accessed 30 June 2023.

[158] Ministry General Secretariat of the Presidency, Ministry of Economy, Development, and Tourism, and Ministry of Finance, '11144-07 Merged with 11092-07: It regulates the protection and processing of personal data and creates the Agency for the Protection of Personal Data.' (*Honourable Chamber of Deputies of Chile*, 15 March 2017) <https://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=11661&prmBoletin=11144-07> accessed 30 June 2023.

[159] Amendment to Article 19 N° 4 via Law No. 21.096 (16 June 2018)

In response to a request from the Undersecretariat of Telecommunications (SUBTEL) for telecommunications companies to provide SUBTEL with sizable amounts of personal user data, the Chilean Transparency Council (CPLT) issued a statement on August 6th, 2020.[160]

The CPLT observed that SUBTEL issued a communication to corporations soliciting the submission of customer data for the purpose of conducting an opinion survey. Additionally, the CPLT noted that a company that has been granted a contract for the establishment of a technical standard for internet access and minimum internet speed will be accountable for the collection of user data through software that may be installed on mobile devices or computers to measure speed. This software will gather and transmit personal data to SUBTEL.[161]

The CPLT stipulated that adherence to the principles of necessity and proportionality is imperative. The collection and utilisation of data should be limited to the intended purposes, and only essential information should be gathered. This is in accordance with the provisions of Law No. 19.628 on the Protection of Private Life, 1999.[162]

In addition, the CPLT emphasised the importance of adhering to global standards and norms regarding this matter and drew attention to a recent legislative proposal being deliberated in Parliament, which aimed to update the existing legal framework and address any deficiencies.

The Personal Data Protection Act (Law No. 19.628) is a significant legislative instrument that establishes guidelines pertaining to the collection, processing, and storage of private data.[163] The important sections of the Act establish the concept of private data, mandate the obtaining of informed consent for the handling of such data, and provide individuals with the entitlement to access, correct, and delete their private data.

---

[160] Council for Transparency, 'CPLT questions that SUBTEL asks for personal data of users to telecommunications companies.' (*CPLT*, 06 August 2020) <https://www.consejotransparencia.cl/cplt-cuestiona-que-subtel-pida-datos-personales-de-usuarios-a-empresas-de-telecomunicaciones/> accessed 30 June 2023.

[161] ibid.

[162] Macarena Gatica and Jaime Urzua, 'Chile - Data Protection Overview.' (*OneTrust LLC*, 30 November 2022) <https://www.dataguidance.com/notes/chile-data-protection-overview> accessed 30 June 2023.

[163] Ministry General Secretariat of the Presidency, 'Law 19628: On the Protection of Privacy.' (Promulgation: 18 August 1999, Publication: 28 August 1999, Last Modified: 10 November 2022 - Law 21504)

Furthermore, the legislation highlights the responsibility to enforce protective measures that ensure the confidentiality, integrity, and availability of personal information, thereby preventing unauthorised access, modification, or disclosure.

The Data Protection Agency, created in accordance with Law No. 19.628, is essential to enforcing adherence to data protection laws. It confers authority to enforce data protection obligations, and it empowers the regulatory body to investigate infractions and levy penalties, including monetary fines and sanctions.

The Cyber Security Law, proposed by President Piñera in one of his final official actions, is presently under deliberation in Congress.[164] The proposed legislation aims to establish a system of protection and protocols for Chile, its network, data, and infrastructure, as well as for private entities that are considered owners of critical infrastructure, such as utility companies and transportation providers.[165]

Additionally, the legislation aims to strengthen national security in the context of cyber-related events. It aims to mitigate potential security breaches and establish appropriate protocols to ensure the uninterrupted operation of businesses and the safeguarding of sensitive information.

The regulation entails specific responsibilities for those who are subject to it, including the requirement to uphold a record of all activities, execute a plan for business continuity, conduct regular monitoring and assessment of their procedures, perform drills to prepare for cyber-attacks, and other related obligations.

The proposed legislation includes provisions for the establishment of a National Agency for Cyber Security.[166] The primary objective of this agency would be to provide guidance to the President on matters related to cybersecurity as well as to collaborate in safeguarding cyberspace.

Additionally, the agency would be responsible for monitoring and overseeing compliance with the new law by both public and private entities, among other duties. At present, the Bill is under deliberation in the Senate and is pending expert evaluations prior to the voting process for the proposed legislation.

---

[164] Andrés Amunátegui Echeverría, 'New bill on cyber security in Chile.' (*Lexology*, 20 July 2022) <https://www.lexology.com/library/detail.aspx?g=efc2cfc3-f084-478f-8359-28aba97e1e41> accessed 30 June 2023.
[165] ibid.
[166] ibid.

Despite not being a member of the European Union, Chile recognises the importance of conforming its data protection laws to global benchmarks. Chilean legislation has integrated principles like those of the General Data Protection Regulation (GDPR), with a focus on transparency, consent, and the rights of data subjects.

In summary, Chile has implemented noteworthy measures to safeguard personal data and guarantee data confidentiality in response to the phenomena of surveillance capitalism and digital colonialism. Chile places a high priority on transparency, consent, and the rights of data subjects by implementing comprehensive legal frameworks, policies, and regulations such as the Personal Data Protection Act, the Digital Rights Protection Act, the Cybersecurity Law, and the GDPR.

The enforcement of compliance and protection of data privacy are critical functions carried out by the Data Protection Agency. The swift advancements in technology necessitate a continuous evolution of Chile's legal frameworks to adequately tackle emerging challenges and offer substantial safeguarding for individuals' data.

4.4. LEGAL AND REGULATORY FRAMEWORK IN NIGERIA

Nigeria has instituted various legal frameworks, policies, and regulations to safeguard personal data and uphold privacy rights, especially in the backdrop of surveillance capitalism and digital colonialism.

A key piece of legislation in this respect is the National Information Technology Development Agency (NITDA) Act,[167] which designates the NITDA as the nation's top IT regulatory body. The Act confers upon the National Information Technology Development Agency (NITDA) the authority to create rules, regulations, frameworks, and standards of practise that are geared towards safeguarding private data and privacy.[168]

The National Information Technology Development Agency (NITDA) established the Nigeria Data Protection Regulation (NDPR) in 2019,[169] which is a notable initiative in Nigeria. The National Data Protection Regulation (NDPR) offers a comprehensive legal structure for safeguarding data across the nation. The document sets forth

[167] National Information Technology Development Agency Act 2007, Act No. 28, published in the Federal Republic of Nigeria Official Gazette No. 99 Vol. 94 Lagos, 05 October 2007.
[168] National Information Technology Development Agency Act 2007, s 6.
[169] The National Information Technology Development Agency Act 2007, s 6 (a)and (c).

fundamental guidelines for safeguarding data, including but not limited to fair and lawful processing, limiting data usage to specific purposes, ensuring data accuracy, and implementing security measures.

The significance of acquiring informed authorization from individuals for the handling of their personal data is underscored in NDPR.[170] The regulation also confers upon individuals the entitlement to access and rectify their personal data retained by data controllers, thereby endowing them with authority over their information.[171]

To adhere to data protection regulations, the Nigerian Data Protection Regulation (NDPR) requires that Data Protection Officers (DPOs) be designated within essential organisations.[172] The Data Protection Officers (DPOs) bear the responsibility of ensuring that the processing of data conforms to the principles and obligations stipulated in the Nigerian Data Protection Regulation (NDPR).

According to the NDPR, it is required that Data Protection Officers (DPOs) possess specialised knowledge in the areas of data protection and privacy. This requirement serves to foster an environment of accountability and consciousness within organisations.

The NDPR also addresses the issue of cross-border data transfers. It is required that any transfers of this nature be accompanied by suitable measures to ensure their protection.[173]

In accordance with established protocols, data controllers are obligated to secure the consent of data subjects or verify that the destination country has implemented sufficient measures for safeguarding data. This particular provision serves to ensure the protection of personal data during its transfer beyond national borders, thereby safeguarding the privacy of individuals in the worldwide digital realm.

Apart from the regulations pertaining to data protection, Nigeria has additional laws and policies that serve to safeguard individual data. The Freedom of Information Act (FOIA), which was implemented in 2011, ensures the right to access information and

[170] The Nigeria Data Protection Regulation 2019, reg 2.3.
[171] The Nigeria Data Protection Regulation 2019, reg 3.1.
[172] The Nigeria Data Protection Regulation 2019, reg 4.1. (2).
[173] The Nigeria Data Protection Regulation 2019, reg 2.2.

fosters transparency and responsibility.[174] The provision enables individuals to make requests for access to public records, thereby enhancing transparency and empowering citizens to hold public authorities responsible for the management of personal information.

The Cybercrimes Act, which was enacted in 2015,[175] serves as a pivotal instrument in the fight against cybercrimes that jeopardise the confidentiality of data. The Act makes the act of accessing computer systems and databases without proper authorization a criminal offence.[176] This provision serves to legally safeguard against the unauthorised access, surveillance, and sharing of personal data.

In addition, the Nigerian Communications Commission (NCC) has implemented a Consumer Protection Framework aimed at safeguarding consumer rights within the telecommunications sector.[177] The present framework establishes a set of guidelines for telecommunications operators to follow in their management of personal data. These guidelines encompass the need to obtain consent from data subjects as well as the obligation to report data breaches.[178] Through this process, it fortifies the safeguarding of personal data and amplifies individuals' autonomy over their information.

The introduction of data protection guidelines by the Central Bank of Nigeria (CBN) for financial institutions within the country has also taken place.[179] The guidelines necessitate that financial institutions institute policies and practises pertaining to data protection to ensure the security of customer information and preclude any unauthorised access or disclosure.[180] The Central Bank of Nigeria (CBN) endeavours

[174] Uchechukwu Nwoke, 'Access to Information under the Nigerian Freedom of Information Act, 2011: Challenges to Implementation and the Rhetoric of Radical Change.' (2019) 63(3) Journal of African Law, Cambridge University Press.
[175] The Nigeria Cybercrimes (Prohibition, Prevention, etc) Act, 2015
[176] The Nigeria Cybercrimes (Prohibition, Prevention, etc) Act, 2015, s 14.
[177] Adeyemi Adepetun, 'NCC targets faster resolution of consumer complaints.' (*The Guardian*, 29 July 2020) <https://guardian.ng/business-services/ncc-targets-faster-resolution-of-consumer-complaints/> accessed 30 June 2023.
[178] Adeyemi Adepetun, 'NCC targets consumer protection, infrastructure expansion.' (*The Guardian,* 13 January 2021) <https://guardian.ng/technology/ncc-targets-consumer-protection-infrastructure-expansion/> accessed 30 June 2023.
[179] Central Bank of Nigeria, 'Consumer Protection Framework Guidelines on Disclosure and Transparency.' (*CBN.gov.ng)* <https://www.cbn.gov.ng/Out/2019/CCD/Draft%20Guidelines%20on%20%20Disclosure%20and%20Transparency%20(002).pdf > accessed on 30 June 2023.
[180] Elizabeth Kolade, 'Cybersecurity in Nigeria's Financial Industry: Enhancing Consumer Trust and Security.' (*Carnegie Endowment for International Peace,* 13 May 2022)

to safeguard personal data within the financial sector, which is deemed highly sensitive, by enforcing these prescribed guidelines.

Regardless of the classification of data protection as a fundamental right or a tort under applicable laws, it is subject to judicial review in Nigerian courts.[181] As per the Nigeria Data Protection Regulation (NDPR), individuals who have experienced infringements on their privacy rights have the option to pursue legal action in court without having a detrimental effect on the proceedings of the Administrative Redress Panel (ARP).[182]

The ARP was established under the supervision of the National Information Technology Development Agency (NITDA). Furthermore, the Federal High Court of Nigeria ruled that a person who provided data has the legal right to sue for the violation of their data under the NDPR.[183]

The jurisprudence surrounding data protection in Nigeria is currently lacking in depth, and the higher courts have yet to establish a clear stance on the scope of data protection rights as outlined in the NDPR. This situation has impeded the advancement of the concept within the country. On the other hand, Nigeria has made noteworthy progress in the establishment of legal frameworks, policies, and regulations for data protection.

However, it is crucial to maintain ongoing monitoring and enforcement of compliance. The promotion of a data-driven environment that values privacy and empowers individuals in the context of surveillance capitalism and digital colonialism can be facilitated through awareness campaigns and educational initiatives. By adhering to these principles, Nigeria has the potential to cultivate a digital ecosystem that is both secure and reliable for its populace.

4.5. LEGAL AND REGULATORY FRAMEWORK IN SOUTH AFRICA

South Africa has established various legislative frameworks, policies, and regulations aimed at safeguarding personal data and upholding data privacy amidst the rise of

<https://carnegieendowment.org/2022/05/13/cybersecurity-in-nigeria-s-financial-industry-enhancing-consumer-trust-and-security-pub-87123> accessed 30 June 2023.

[181] Emerging Market Telecommunication Service v Eneye (2018) LPELR 46193(CA)

[182] Nigerian Data Protection Regulation (NDRP) reg. 4.2(1).

[183] Incorporated Trustees of Laws and Rights Awareness Initiative v. National Identity Management Commission (NIMC) Suit No FHC/AB/CS/79/2020.

surveillance capitalism and digital colonialism. The Protection of Personal Information Act (POPIA)[184] is a fundamental legislative measure pertaining to data privacy. It has been fully enforced as of July 1, 2021.

The Protection of Personal Information Act (POPIA) sets forth a framework of guidelines for the legitimate handling of personal data, including the requirement of obtaining consent and adhering to legitimate interests in addition, it confers upon data subjects the privilege to access and rectify their personal data while imposing an obligation upon responsible entities to establish security measures.[185]

The Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA)[186] is deemed a significant piece of legislation. It contains measures that prioritise lawful surveillance while also incorporating clauses that uphold the privacy of communications and prevent misuse[187]. These provisions guarantee that interceptions are sanctioned and monitored, thereby promoting accountability.

The Electronic Communications and Transactions Act (ECTA)[188], enacted in 2002, regulates electronic communications and transactions, thereby playing an indirect role in safeguarding data privacy. The ECTA legislation serves to prohibit the dissemination of unsolicited commercial communications and criminalises any unauthorised access, interception, or interference with computer data.[189] This serves to protect individuals from unwanted direct marketing and unauthorised data access.

South Africa, in addition to specific legislative measures, has implemented the National Cybersecurity Policy Framework (NCPF) as a guiding instrument to

[184] Protection of Personal Information Act (POPI Act) 4 of 2013.
[185] Lee Swales, 'The Protection of Personal Information Act and data de-identification Discussions on POPIA'. (2021) 117(7/8) South African Journal of Science.
[186] Regulation of Interception of Communications and Provision of Communication-related Information Act (RICA) Act 70 of 2002.
[187] Republic of South Africa, 'Documents: Acts: Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002.' (*South African Government Official Portal*) <https://www.gov.za/documents/regulation-interception-communications-and-provision-communication-related-information--13> accessed 30 June 2023.
[188] Electronic Communications and Transactions Act (ECTA) Act 25 of 2002.
[189] Republic of South Africa, 'Documents: Acts: Electronic Communications and Transactions Act 25 of 2002.' (*South African Government Official Portal*) <https://www.gov.za/documents/electronic-communications-and-transactions-act> accessed 30 June 2023.

augment cybersecurity measures and safeguard crucial information infrastructure.[190] Although the NCPF does not exclusively concentrate on data privacy, it underscores the significance of safeguarding personal information in the digital realm and promotes the adoption of privacy controls and data protection mechanisms.

Recently, South African journalist Sam Sole and the AmaBhungane Centre for Investigative Journalism sued in the High Court to declare the Regulation of Interception of Communications and Provision of Communication-Related Information Act, 70 of 2002 (RICA), unconstitutional for failing to protect privacy.[191]

Sole had suspected monitoring and surveillance of his communications in 2008. He asked the Inspector-General of Intelligence about monitoring his communications in 2009. The Inspector-General denied state agency misconduct. However, they failed to verify Sole's communications surveillance.

In 2015, Sole's communication with a state prosecutor was used as evidence in unrelated court cases, confirming Sole's conversations were intercepted in 2008. Sole then requested interception information from the State Security Agency. Sole only got information on two interception authorization renewals, not the legality or logic behind the original request.

The Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA) replaced the Interception and Monitoring Prohibition Act, 127 of 1992, and covered verbal, electronic, and mobile communication. Section 2 of the Act prohibits interception without following appropriate processes. These processes target major crimes, public health and safety, national security and economic interests, organised crime, and terrorism. Surveillance requests were filed ex-parte with a judge chosen by the Minister of Justice without a chance for counterargument.

The High Court case argued that the Regulation of Interception of Communications and Provision of Communication-Related Information Act's (RICA) notification mechanism was inadequate, preventing surveillance subjects from receiving

[190] Republic of South Africa, 'Documents: Notices: National Cybersecurity Policy Framework.' (*South African Government Official Portal,* 04 December 2015) <https://www.gov.za/documents/national-cybersecurity-policy-framework-4-dec-2015-0000> accessed 30 June 2023.

[191] AmaBhungane Centre for Investigative Journalism NPC and Another v. Minister of Justice and Correctional Services and Others; [2021] ZACC 3; 2021 (4) BCLR 349 (CC); 2021 (3) SA 246 (CC) (4 February 2021)

notification and contesting its legality. The selected judge was appointed unilaterally, compromising their independence and failing to offer proper adversarial mechanisms to safeguard the subjects throughout the ex-parte application process.

The lack of data gathering and storage norms and specific safeguards for journalists and attorneys under surveillance has raised concerns. The National Communication Centre's mass interception was unlawful, unauthorised, and unconstitutional.

On September 16, 2019, the North Gauteng High Court declared RICA unlawful. Due to the lack of warning to subjects, ex-parte petitions, and journalist and lawyer surveillance, the court found that the right to privacy was arbitrarily and unreasonably infringed. The court found RICA's data management practises unconstitutional and the National Communication Centre's mass monitoring actions illegal.

The court suspended the declaration of invalidity for two years to give Parliament time to fix the issues. For interim relief, certain temporary remedies have been incorporated into the existing Act.

The collection of policies, rules, and regulations establishes a thorough legal framework aimed at protecting personal data and guaranteeing data confidentiality. Regular monitoring and adjustment of these structures will be imperative to effectively tackle emerging challenges in the rapidly changing digital environment.

Sustained initiatives are essential in maintaining a competitive edge against the practises of surveillance capitalism and digital colonialism while simultaneously preserving the privacy rights of the people in South Africa.

4.6. LEGAL AND REGULATORY FRAMEWORK IN SINGAPORE

Singapore has acknowledged the significance of safeguarding personal data and upholding data confidentiality amidst the growing challenges presented by surveillance capitalism and digital colonialism. In response to these concerns, the government has instituted a comprehensive legal structure, policies, and regulations aimed at protecting the rights of individuals with regards to their data and privacy.

The cornerstone of Singapore's legislative framework for data protection is the Personal Data Protection Act (PDPA). The Personal Data Protection Act (PDPA), which was implemented in 2012 and subsequently revised in 2020, governs the

procedures surrounding the acquisition, utilisation, and disclosure of personal information by corporations[192].

Part 4 is a significant stipulation that necessitates organisations to secure the consent of individuals prior to the collection, utilisation, or disclosure of their personal information[193]. This measure guarantees that individuals retain authority over their data and prohibits organisations from gathering data without appropriate consent.

Apart from the requirement of obtaining consent, according to the Personal Data Protection Act (PDPA)[194], it is mandatory for organisations to provide individuals with information regarding the objectives behind the collection of their private data and to obtain their consent. The clause serves to enhance transparency and deter organisations from gathering information without a valid justification.

Singapore established the Personal Data Protection Commission (PDPC) to address concerns pertaining to digital colonialism and ensure adherence to data protection regulations.[195] The Personal Data Protection Commission (PDPC) is responsible for the oversight and enforcement of the Personal Data Protection Act (PDPA), with the aim of ensuring that organisations comply with the regulations pertaining to data protection. The Personal Data Protection Commission (PDPC) offers guidance and advisory viewpoints to entities, encouraging ethical data handling and cultivating a climate of data confidentiality.[196]

To address the issue of digital colonialism, the Act prohibits entities from transferring private data to countries that do not offer equivalent data protection measures.[197] This provision serves as a protective measure to prevent the exploitation of personal data by foreign corporations that operate under less stringent regulations. Singapore's regulations on data transfers serve as a safeguard to ensure the protection of individuals' personal data, even in cases where it is shared with foreign entities.

---

[192] Personal Data Protection Commission, 'PDPA Legislation Overview.' (*PDPC Singapore Government Agency*) <https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation> accessed 30 June 2023.

[193] Personal Data Protection Act 2012, Part 4: Collection, Use and Disclosure of Personal Data, s 13 to s 20.

[194] Personal Data Protection Act 2012, s 13.

[195] Personal Data Protection Commission, 'PDPC: Who we are' (*PDPC Singapore Government Agency*) <https://www.pdpc.gov.sg/Who-We-Are> accessed 30 June 2023.

[196] Personal Data Protection Commission, 'PDPC: Advisory Committee' (*PDPC Singapore Government Agency*) < https://www.pdpc.gov.sg/Who-We-Are/Advisory-Committee > accessed 30 June 2023.

[197] Personal Data Protection Act 2012, s 26.

To enhance the safeguarding of data privacy, the government of Singapore adopted additional rules and regulations. The Trusted Data Sharing Framework (TDSF), which was introduced in 2021, enables the secure and regulated sharing of data while safeguarding the privacy of individuals.[198] The implementation of data protection measures is mandatory for organisations under the TDSF, with the aim of ensuring sufficient protection of personal data exchanged between entities.

The Cybersecurity Act (CSA)[199] is a pivotal component in the protection of data privacy from the threats of surveillance capitalism and digital colonialism. The Cyber Security Agency of Singapore (CSA) is authorised under the Act to conduct investigations and take measures to address cybersecurity risks, which may encompass incidents such as data breaches.[200]

The CSA possesses the jurisdiction to implement and uphold data protection protocols and establish benchmarks for safeguarding private data, thereby guaranteeing the protection of personal information.

The certification programme known as the Data Protection Trustmark (DPTM) has been recently introduced by the InfoComm Media Development Authority (IMDA).[201] Entities that acquire DPTM certification exhibit adherence to data protection stipulations. The Data Protection Trust Mark (DPTM) serves to enhance the confidence of individuals in organisations by providing assurance that their personal data is being handled in a secure and compliant manner with data protection regulations.

The Singapore Court of Appeal (SGCA) delivered a noteworthy judgement that upholds the significance of safeguarding personal data in Singapore. The Court expounded on the scope of the right to private action as stipulated under the Personal Data Protection Act 2012 (PDPA)[202].

---

[198] The InfoComm Media Development Authority (IMDA) and Personal Data Protection Commission (PDPC), 'Enabling Data-Driven Innovation Through Trusted Data Sharing in a Digital Economy.' (*IMDA Singapore Government Agency*, 28 June 2019) <https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/archived/imda/press-releases/2019/enabling-data-driven-innovation-through-trusted-data-sharing-in-a-digital-economy> accessed 30 June 2023.
[199] Cybersecurity Act 2018 (No. 9 of 2018).
[200] Cybersecurity Act 2018, s 15.
[201] The InfoComm Media Development Authority (IMDA), 'Official Launch of Data Protection Trustmark' (*IMDA Singapore Government Agency*, 09 January 2019) <https://www.imda.gov.sg/-/media/Imda/Files/Programme/DPTM/DPTM-Information-Kit.pdf > accessed 30 June 2023.
[202] Personal Data Protection Act 2012, s 32(1).

The case of Reed v. Bellingham[203] resulted in a ruling by the SGCA that emotional distress meets the criteria of 'loss or damage' necessary for initiating a private action under Section 32(1) of the PDPA. This decision overturned the previous ruling made by the Singapore High Court.

In this case, Mr. Alex Bellingham unlawfully gathered and utilised Mr. Michael Reed's personal data, a client of his former company. After leaving his previous job to join a competing company, Mr. Bellingham used his personal email account to communicate with Mr. Reed, sharing information about his former employer's investment activities and offering new investment opportunities. Mr. Bellingham ignored Mr. Reed's concerns about the gathering and storage of his private data.

Mr. Reed sued Mr. Bellingham in District Court under PDPA Section 32(1). Mr. Bellingham was ordered to delete all of Mr. Reed's personal data by the district court. On appeal, the High Court reversed these orders. The High Court ruled that Mr. Reed's mental anguish and loss of control over personal data did not constitute 'loss or damage' under Section 32(1) of the PDPA.

On appeal, The Court upheld Mr. Reed's appeal, affirmed the District Judge's decisions, and issued the injunction and order to erase his personal data.

The case of *Reed v. Bellingham* serves as a compelling example of the significance attributed to safeguarding private data in Singapore. The Singapore Personal Data Protection Commission (PDPC) places significant importance on Parliament's intention to establish strong safeguards for individuals' personal data. This emphasis is reflected in the court's willingness to support this objective, suggesting that Singapore's personal data framework will continue to evolve and become more robust in the future.

In a nutshell, Singapore has established a comprehensive legal framework, rules, and regulations aimed at safeguarding personal data and upholding data privacy amidst the prevalence of surveillance capitalism and digital colonialism. The protection of data privacy and the promotion of responsible data practises are facilitated by several regulatory measures, including but not limited to the Personal Data Protection Act (PDPA), the Trusted Data Sharing Framework, the Cybersecurity Act, the Data

[203] Reed, Michael v Bellingham, Alex (Attorney-General, intervener) [2022] SGCA 60.

Protection Trustmark certification programme, and the Personal Data Protection Commission.

The all-encompassing strategy adopted by Singapore can be considered a paradigm for other countries that are confronted with comparable issues. This approach highlights the significance of maintaining a harmonious equilibrium between innovation, data exchange, and individual privacy.

4.7. LEGAL AND REGULATORY FRAMEWORK IN MALAYSIA

Malaysia has undertaken noteworthy measures in safeguarding personal data and upholding data confidentiality in recent times, considering apprehensions regarding surveillance capitalism and digital colonialism. The Personal Data Protection Act 2010 (PDPA)[204] is the primary legislation that regulates data protection matters in Malaysia. The PDPA is based on the EU directive,[205] resulting in the principles and requirements outlined in the PDPA being largely comparable to the data protection requirements established in the UK's Act of 1998.[206]

It is worth noting that there are several significant distinctions between the data protection laws of the European Union (EU) and the Personal Data Protection Act (PDPA). These differences include, but are not limited to, the fact that (1) the PDPA solely pertains to the processing of private data in commercial operations; (2) the PDPA does not apply to both the national and state governments; (3) the PDPA does not explicitly grant data subjects the right to initiate legal proceedings for a violation of their PDPA-related rights; and (4) the Commissioner is accountable to a minister instead of to parliament.

The Personal Data Protection Act (PDPA) lays down a set of principles and regulations aimed at safeguarding personal data and ensuring that organisations responsible for handling such data comply with the established guidelines. The Act furnishes definitions for important terminologies, including but not limited to personal data, data user, data subject, and sensitive personal data.[207]

[204] Personal Data Protection Act (PDPA) Act 709 of 2010.
[205] European Union Data Protection Directive 95/46/EC.
[206] Data Protection Act 1998 c. 29.
[207] Personal Data Protection Act 2010, s 3.

The Act defines fundamental principles that data users are obligated to comply with, which encompass acquiring consent for data processing, confining data collection to essential purposes, and guaranteeing data security.[208] It provides data subjects with distinct rights, including but not limited to the right to access, rectify, and revoke consent for their own private data.[209] It establishes the data protection principles that data users have a duty to adhere to, with a particular emphasis on the accuracy and preservation of personal data.[210]

The safeguarding of personal data in Malaysia is also attributed to the Communications and Multimedia Act (CMA) of 1998.[211] The legislation encompasses numerous aspects of information and communication technology, notably the safeguarding of individuals' personal information. The Act stipulates that the act of accessing computer systems without proper authorization is prohibited, thereby serving as a protective measure against unsanctioned surveillance of personal data.[212]

Furthermore, the Act guarantees the confidentiality of communications that are transmitted through networks, thereby safeguarding the privacy of individuals' digital interactions.[213]

Malaysia has taken measures to address the issue of cybersecurity by enacting laws and regulations aimed at mitigating digital threats and safeguarding personal information. The Computer Crimes Act of 1997[214] criminalises the unauthorised access, interception, and misuse of computer systems, thereby establishing protective measures against unauthorised access and surveillance of personal data.

The Digital Signature Act of 1997[215] holds significant importance in upholding the genuineness and reliability of electronic communications and transactions through the provision of legal acknowledgement for digital signatures.

Malaysia has developed a national cybersecurity policy and several strategies to comprehensively tackle cybersecurity concerns. The initiatives are geared towards enhancing cybersecurity competencies, fostering consciousness, and engaging with

[208] Personal Data Protection Act 2010, s 4.
[209] Personal Data Protection Act 2010, s 7.
[210] Personal Data Protection Act 2010, s 9.
[211] Communications and Multimedia Act (CMA) Act 588 of 1998.
[212] Communications and Multimedia Act 1998, s 140 and s 167.
[213] Communications and Multimedia Act 1998, s 63.
[214] Computer Crimes Act (CCA) Act 563 of 1997.
[215] The Digital Signature Act (DSA) Act 562 of 1997.

relevant parties to ensure the protection of data privacy. The National Cybersecurity Policy functions as a guiding structure for safeguarding individual data and expanding secure digital conduct.[216]

In Malaysia, there are regulations that are specific to certain sectors and are designed to safeguard the privacy and confidentiality of personal data. The Financial Services Act[217] and the Islamic Financial Services Act[218] are regulatory measures that oversee the gathering, handling, and disclosure of financial data, thereby safeguarding confidentiality within the financial industry.

Additionally, there exists a proposed legislation known as the Health Data Protection Act, which seeks to safeguard health-related personal data and oversee its acquisition, retention, and dissemination within the healthcare industry.

The High Court's grounds of judgement for the Genting case were made public in December 2021.[219] This marked the first instance where Malaysian courts adjudicated a formal challenge against government authorities regarding their authority to demand the release of personal data under the Personal Data Protection Act (PDPA).

The ruling of the High Court effectively imposed restrictions on the data collection powers of enforcement and regulatory bodies. The High Court ruled that, despite the exemptions outlined in the PDPA, regulatory agencies are not permitted to request the unrestricted disclosure of private data from users.

To summarise, Malaysia has established various legal frameworks, policies, and regulations aimed at safeguarding personal data and upholding data privacy amidst the prevalence of surveillance capitalism and digital colonialism. Malaysia endeavours to safeguard individual data rights and foster a secure and reliable digital environment for its populace by means of persistent evaluation and enhancement of these measures.

The Personal Data Protection Act, the Communications and Multimedia Act, cybersecurity laws, national cybersecurity policies, and sector-specific regulations are

[216] Mohd. Shamir b Hashim, 'Malaysia's National Cyber Security Policy: The country's cyber defence initiatives.' (2011) Proceedings of the Second Worldwide Cybersecurity Summit (WCS), IEEE Conference Proceeding, London, UK.
[217] The Financial Services Act (FSA) Act 758 of 2013.
[218] The Islamic Financial Services Act (IFSA) Act 759 of 2013.
[219] Genting Malaysia Berhad v. Personal Data Protection Commissioner & Ors. Case No. WA-25-83-02/2020.

just a few examples of the legislative measures that demonstrate Malaysia's commitment to protecting personal data.

To sum up, power disparities, economic interdependencies, and historical events all play a role in how governments and policymakers in the global South engage with the phenomena of digital colonialism and surveillance capitalism. The nations situated in the Global South, characterised by their sizable populations and burgeoning digital landscapes, have emerged as profitable markets for the practise of surveillance capitalism.

Nevertheless, policymakers in these areas frequently encounter difficulties reconciling economic progress with safeguarding privacy and individual rights. The analysis of legal frameworks provides insight into the strategies employed by governments in tackling the obstacles presented in regards to privacy laws and the rights of individuals.

The overarching objective ought to be to foster equitable and comprehensive digital progress, empowering the emerging nations of the southern hemisphere to proactively shape their digital trajectory while safeguarding the entitlements and welfare of their populace. Through a comprehensive analysis and targeted intervention, policymakers can endeavour to achieve a digital environment that is more just and harmonious in the developing regions of the world.

CHAPTER 5

FINDINGS, CONCLUSION AND SUGGESTIONS

5.1. CONCLUSION

The research explored the concepts of data colonialism, data sovereignty, surveillance capitalism, and subjugated society in the context of the digital age.

Data colonialism refers to the exploitative relationship between the Global North and the Global South, where valuable data is extracted from the latter and controlled by dominant tech companies. Data sovereignty, on the other hand, emphasises ownership, control, and local infrastructure to counter data colonialism.

Surveillance capitalism, coined by Shoshana Zuboff, is a form of capitalism that revolves around the extraction, analysis, and commodification of personal data. It erodes privacy, undermines individual autonomy, and consolidates power and wealth in the hands of a few tech corporations. Zuboff calls for a new social contract that prioritises individual sovereignty and democratic oversight of data practises.

Subjugated society highlights how surveillance technologies are used by authoritarian states to oppress minority groups based on race, ethnicity, religion, nationality, political affiliation, or social participation. The state, often in collaboration with corporations, utilises surveillance to maintain power, discriminate, and suppress dissent. Overall, these issues reveal the complex dynamics and ethical challenges of the digital era.

Achieving a fair and equitable data landscape requires addressing power imbalances, protecting privacy rights, fostering transparency and accountability, and reimagining the relationship between individuals, governments, and tech corporations. It calls for international cooperation, ethical data practises, and the development of legal and regulatory frameworks that protect individual rights and promote a more inclusive and democratic digital society.

The research further sheds light on the pervasive influence of multinational corporations in the realms of surveillance capitalism and digital colonialism. The examples and legal cases discussed illustrate the significant impact these corporations

have on data privacy, user rights, and market dynamics. Companies such as Google, Facebook, Amazon, Meta IE, and Microsoft have amassed vast amounts of user data, sometimes without explicit consent, leading to concerns about privacy breaches and the unethical use of personal information.

Instances such as the Cambridge Analytica scandal and security breaches at Microsoft highlight the urgent need for robust data protection measures and ethical practises by these corporations. The enforcement actions taken by regulatory authorities, such as the fines imposed by the EDPB on Meta IE, underscore the importance of compliance with data protection laws and the potential consequences for non-compliance.

Moreover, the extraterritorial scope of warrants and the global access to digital communications granted by legislation like the CLOUD Act raise significant questions about privacy rights and the jurisdictional reach of governments. These issues underscore the ongoing tension between individual privacy and government surveillance in the digital age.

In an increasingly interconnected world, striking a balance between technological innovation, corporate interests, and individual rights is crucial. By doing so, we can navigate the evolving landscape of digital technology in a way that respects privacy, promotes fair competition, and empowers individuals in the digital realm.

In conclusion, the phenomenon of digital colonialism and surveillance capitalism presents significant challenges for governments and policymakers worldwide, particularly in the Global South. These countries, with their large populations and expanding digital landscapes, are attractive markets for surveillance capitalism practises. However, policymakers in these regions face the complex task of balancing economic progress with protecting privacy and individual rights.

To address these challenges, governments in the Global South have implemented comprehensive legal frameworks, policies, and regulations aimed at safeguarding personal data and upholding data privacy. Countries in Asia, Africa, and South America have established robust legislative measures, such as the Personal Data Protection Acts, to ensure the responsible handling of personal information by organisations. They have also enacted laws specific to certain sectors, such as the financial and healthcare industries, to protect the confidentiality of sensitive data.

Additionally, countries have introduced cybersecurity laws and strategies to mitigate digital threats and protect personal information from unauthorised access and surveillance. National cybersecurity policies serve as guiding structures for enhancing cybersecurity competencies and fostering awareness among individuals and relevant stakeholders.

While these efforts demonstrate a commitment to protecting personal data and promoting data privacy, policymakers must continue to evaluate and enhance these measures to keep pace with evolving technologies and new challenges. The ultimate goal should be to foster equitable and comprehensive digital progress, empowering emerging nations in the Global South to shape their digital trajectories while safeguarding the rights and welfare of their citizens.

By conducting in-depth analyses and implementing targeted interventions, policymakers can strive to create a digital environment that is fair, just, and harmonious in the developing regions of the world. It is crucial to strike a balance between innovation, data exchange, and individual privacy, ensuring that the benefits of the digital age are accessible to all while preserving the rights and dignity of individuals.

5.2. FINDINGS

The following are the study's outcomes which were reached after examining and discussing numerous objectives in the earlier chapters:

5.2.1. To conduct a critical analysis of the concepts of digital colonialism and surveillance capitalism.

The concepts of surveillance capitalism and data sovereignty provide insight into the workings of the digital economy and the obstacles it presents to privacy, autonomy, and democracy. The concept of data sovereignty pertains to the notion that both individuals and organisations ought to possess authority and jurisdiction over their respective data. Conversely, surveillance capitalism encompasses the act of extracting and capitalising on personal data for the purposes of financial gain and influence.

Data sovereignty presents various strategies to mitigate data colonialism, a phenomenon characterised by the hegemony of a handful of foreign technology corporations over the digital economies of nations in the Global South. The first point

of emphasis is on the ownership and control of data by its creators, which facilitates resistance against external exploitation.

The implementation of legal frameworks and regulations is of paramount importance in safeguarding data and guaranteeing its regulated utilisation. The frameworks in question may encompass a range of legal provisions, such as those pertaining to data protection, privacy, and intellectual property.

The establishment of indigenous data infrastructure, such as data centres and cloud services, diminishes reliance on foreign entities and alleviates the threat of data colonialism. The implementation of data localization policies, which mandate the storage and processing of data within a particular jurisdiction, serves to reinforce data sovereignty by ensuring that data remains subject to the authority of its country or organisation of origin. Finally, the promotion of empowerment and collaboration among stakeholders serves to mitigate the power differentials that are inherent in the phenomenon of data colonialism.

In contrast, surveillance capitalism pertains to the process of acquiring, scrutinising, and commercialising extensive quantities of personal information from individuals within the digital domain. Technology firms and digital platforms acquire information by means of online inquiries, social media engagements, and mobile phone usage, thereby generating comprehensive profiles of individuals' conduct and inclinations.

Subsequently, these observations are utilised to construct prognostic models and customised promotional mechanisms that influence the decisions and conduct of individuals. The novel iteration of capitalism in question regards human life as a commodity that can be traded, thereby diminishing the concepts of privacy and individual autonomy and subverting the fundamental tenets of democracy.

The practise of surveillance capitalism is heavily dependent on the utilisation of big data, which encompasses the collection, retention, and examination of extensive centralised repositories housing data pertaining to internet users on a global scale. The utilisation of this data is aimed at forecasting the future conduct of individuals, which requires extensive monitoring.

The utilisation of big data raises concerns regarding the infringement of individual privacy, as it involves the extraction and commercialization of personal information.

The perpetuation of tech corporations' authority and the fostering of dependency in the Global South due to the dominance of the Global North in the digital ecosystem result in economic and moral disadvantages for these regions.

In the context of societies that are subjugated, the phenomenon of surveillance capitalism assumes a more repressive character. The utilisation of surveillance technologies by the state results in the establishment of a policing system that selectively focuses on and subjugates minority groups based on distinct identification criteria, including but not limited to race, religion, nationality, political ideology, and participation in social groups.

Digital surveillance is employed in authoritarian regimes to monitor and repress individuals or groups that are deemed to pose a risk to the regime's authority. Surveillance enables the state to convert individuals into an abundant source of data, while corporations are instrumental in the advancement of surveillance techniques.

The concept of a subjugated society sheds light on various significant facets of digital surveillance. The statement illustrates the potential justification of surveillance measures on grounds other than race, such as religious affiliation or sexual orientation. The digital surveillance technology utilised in authoritarian regimes is specifically engineered to differentiate and segregate individuals based on their identities, thereby singling out and detecting minority ethnic communities.

The capacity for subjugated societies to resist surveillance is constrained by the imposition of severe penalties for engaging in resistance strategies. Individuals residing in authoritarian states experience limited security and privacy as they are devoid of the constitutional protections that are available in democratic societies.

To summarise, the concepts of surveillance capitalism and data sovereignty bring attention to the intricate matters pertaining to privacy, autonomy, and democracy in the era of digital technology. The concept of data sovereignty presents a set of measures that can be employed to counteract the effects of data colonialism. These measures include prioritising ownership, establishing appropriate legal frameworks, investing in local infrastructure, implementing data localization strategies, and promoting empowerment.

Surveillance capitalism is a phenomenon whereby personal data is utilised for commercial gain, resulting in the erosion of privacy and autonomy. This practise also contributes to the concentration of power and wealth in the hands of dominant technology corporations. The use of surveillance technologies by the state to manage and repress specific groups is exemplified by subjugated societies, thereby highlighting the oppressive character of surveillance. Comprehending these concepts is imperative to tackling the obstacles and endeavouring towards a just and impartial digital terrain.

5.2.2. To analyse the historical and structural elements that have played a role in the emergence of the digital divide between the Global North and South.

The digital divide between the Global North and South has arisen due to a confluence of historical and structural factors that have impacted the evolution and availability of digital technologies. The present study examined significant historical occurrences and structural components that played a role in the creation of this division.

Throughout history, colonisation has exerted a substantial influence on the worldwide economic terrain and laid the foundation for the digital divide. In the period of colonialism, European nations exerted economic and political control over their colonies situated in Africa, Asia, and Latin America.

The exploitative character of colonisation led to the extraction of resources, wealth, and labour from the colonies, thereby leaving them in a state of economic disadvantage. Historical circumstances have established the fundamental basis for the structural disparities that endure in contemporary times, encompassing the digital divide.

The digital divide is partly attributable to a structural element, namely the uneven allocation of economic resources and advancement between the Global North and South. Historically, nations situated in the Global North, such as Western European countries and the United States, have enjoyed superior access to infrastructure, capital, and technological innovations.

The benefit has facilitated their capacity to allocate resources towards the enhancement and establishment of resilient information and communication

technology (ICT) industries, resulting in the widespread adoption of digital technologies and connectivity.

By way of contrast, numerous nations situated in the Global South encounter obstacles that pertain to restricted financial means, insufficient infrastructure, and political instability, thereby impeding their capacity to cultivate and embrace digital technologies.

A further structural element pertains to the inequitable availability of education and levels of literacy. The acquisition of knowledge and skills through education is a crucial factor in determining the level of digital inclusion among individuals, as it enables them to proficiently utilise and derive advantages from digital technologies.

Nonetheless, there are still discrepancies in educational opportunities between the regions of the Global North and South. Numerous nations situated in the Global South encounter various obstacles, including insufficient educational infrastructure, a scarcity of proficient educators, and elevated rates of student attrition. The circumstance impedes the advancement of competencies in digital literacy and sustains the gap in access to digital resources.

The digital divide is significantly impacted by infrastructure and connectivity factors. The accessibility of dependable and reasonably priced internet infrastructure is imperative for the utilisation of digital technologies and engagement in the digital marketplace. Advanced telecommunications networks and expanded internet connectivity have been significantly invested in by developed countries located in the Global North.

By way of contrast, numerous nations situated in the Global South encounter obstacles such as inadequate infrastructure development, exorbitant expenses associated with internet accessibility, and geographical impediments that impede connectivity in rural and secluded regions.

The digital divide has been additionally influenced by political and regulatory factors. In certain cases, ICT development has not been prioritised, and resource allocation has been hindered by competing social and economic priorities within governments in the Global South.

Furthermore, the regulatory frameworks that oversee the Information and Communication Technology (ICT) industry have the potential to either facilitate or impede the process of digital inclusion. Policies that facilitate competition, innovation, and affordability have the potential to mitigate the digital divide, whereas regulations that are restrictive and practises that are monopolistic in nature may further aggravate it.

The impact of multinational corporations represents a significant determinant of the digital divide phenomenon. A considerable number of the leading technology corporations are situated in developed regions of the world and wield substantial influence over the digital landscape.

Frequently, these corporations give precedence to markets in industrialised nations, leading to restricted investment and backing for digital infrastructure and amenities in regions classified as the Global South. In addition, the exorbitant expenses associated with proprietary software and hardware may present impediments to entry for both individuals and institutions situated in developing nations.

Moreover, the partiality in language and content within digital technologies has the potential to sustain the digital divide. The prevalence of English as the dominant language in digital platforms and content creates barriers to access for individuals who do not speak or have limited proficiency in English, particularly in regions where English is not widely spoken or taught.

Insufficient provision of region-specific content and services in vernacular languages can impede digital inclusivity and curtail the prospective advantages of digital technologies for individuals and communities in developing nations.

The digital divide that exists between the Global North and South is a multifaceted matter that is shaped by a confluence of historical and structural elements, as evidenced by the preceding analysis.

The establishment of unequal power dynamics and economic disparities, as well as the presence of structural elements such as limited access to education, inadequate infrastructure, and regulatory challenges, have been perpetuated by historical events such as colonisation. These factors continue to contribute to the existing divide. A comprehensive approach is necessary to tackle the issue of the digital divide.

5.2.3. To examine the strategies used by multinational corporations to leverage their influence and gather information from users in the Global South.

The influence of multinational corporations (MNCs) on surveillance capitalism and digital colonialism is noteworthy, as they are transforming the landscape of technology and the digital economy in unprecedented manners.

The prevalence of major technology firms, primarily situated in the United States, such as Google, Facebook, and Amazon, has enabled them to leverage their technological expertise, financial resources, and market dominance to obtain valuable user information and establish authority within the digital marketplace. By doing so, they have expanded their worldwide impact, affecting user conduct, data gathering methodologies, and market trends in numerous developing nations situated in the Global South.

A key approach utilised by multinational corporations involves the procurement of substantial quantities of user data, frequently without explicit user authorization, with the aim of generating informative profiles and datasets that can be marketed to advertisers. This strategy allows multinational corporations to generate revenue from user data and optimise advertising efforts with greater efficiency.

The Cambridge Analytica scandal, which involved Facebook, is a noteworthy example of the unethical acquisition of personal data for financial benefit. The present instance involves the acquisition of personal data belonging to millions of users without their explicit consent, which was subsequently utilised to achieve political objectives. This serves to underscore the degree to which multinational corporations can leverage data to further their own interests.

Multinational corporations utilise diverse strategies to collect data from users residing in the Global South. Initially, they utilise their dominant position in the market and financial resources to offer digital services and products that are tailored to meet the distinct requirements and inclinations of users in these localities. Multinational corporations (MNCs) can potentially increase their user base and gather significant data on user behaviours, interests, and demographics by providing customised features, language support, and localised content.

Moreover, multinational corporations frequently engage in partnerships with indigenous enterprises and governmental bodies in developing regions of the world with the aim of acquiring user data. Multinational corporations (MNCs) can engage in collaborative efforts with telecommunications companies, internet service providers, and local technology firms to leverage pre-existing data streams and broaden their data acquisition endeavours. Multinational corporations can acquire a diverse array of data by means of such collaborative ventures, encompassing patterns of internet usage, interactions on social media platforms, and information pertaining to mobile devices.

Multinational corporations often adopt the approach of offering digital services and platforms at a reduced cost or free of charge as a means of achieving their objectives. Multinational corporations (MNCs) can expand their user base in the Global South by providing various products, including free email services, social networking platforms, and messaging applications. Notwithstanding, these services frequently entail a compromise: users furnish personal information in return for admission to these platforms. The aforementioned data is subsequently employed for the purpose of targeted advertising, algorithmic profiling, and other forms of monetization.

In addition, multinational corporations (MNCs) proactively participate in the practise of data mining and algorithmic analysis as a means of extracting valuable insights from the extensive quantities of data they accumulate. Sophisticated data analytics methodologies empower these enterprises to detect patterns, tendencies, and associations in user conduct, inclinations, and consumption practises.

This information is subsequently utilised to enhance their offerings, customise user interactions, and optimise their promotional tactics. Through consistent refinement and enhancement of their algorithms, multinational corporations can sustain their competitive edge and uphold their dominance within the digital marketplace.

Multinational corporations may utilise their platforms to exert influence over user behaviours and preferences in certain instances. Multinational corporations (MNCs) can influence user decisions by utilising meticulously crafted user interfaces, recommendation systems, and content algorithms to direct them towards particular products, services, or information. The ability to regulate user experiences provides

multinational corporations with the opportunity to augment their data acquisition endeavours and reinforce their market standing.

In order to mitigate the impact and tactics utilised by multinational corporations, it is imperative to implement comprehensive and ethical strategies that safeguard individual rights, foster equitable competition, and redress power imbalances.

It is imperative for governments and regulatory bodies to establish stringent data protection policies and implement them with efficacy in order to safeguard user privacy and uphold consent. The regulations ought to mandate explicit consent from users for the purpose of data collection, ensure transparency and control over user data, and enforce severe penalties for non-compliance.

Facilitating competition within the digital realm is imperative in order to deter the monopolistic behaviours exhibited by multinational corporations (MNCs). It is recommended that governments promote the growth of domestic technology sectors, provide assistance to indigenous startups, and cultivate creativity via regulations that facilitate equitable market competition. Furthermore, advocating for open-source software, decentralised platforms, and data ownership models that enhance user empowerment can serve as a means to mitigate the hegemony of multinational corporations and offer alternative choices for users residing in the developing regions of the world.

The promotion of education and digital literacy programmes is crucial in enabling users residing in the Global South to be empowered. Empowering individuals with the requisite knowledge and competencies to comprehend data privacy concerns, make judicious decisions, and safeguard their digital entitlements can enhance their resilience against the tactics employed by multinational corporations. The implementation of awareness campaigns, digital literacy programmes, and initiatives aimed at promoting responsible data usage can have a substantial impact on the empowerment of individuals and communities.

To sum up, the techniques employed by multinational corporations to exploit their sway and collect data from users in the developing regions of the world are intricate and diverse. The aforementioned instances, in conjunction with legal precedents and controversies, emphasise the necessity for all-encompassing and morally sound tactics to protect personal liberties, promote equitable competition, and tackle power

imbalances that stem from the dominance of multinational corporations in the digital realm.

It is feasible to establish a digital environment that is more equitable and respects privacy by implementing stringent data protection policies, fostering competition, and equipping users with knowledge and proficiency in digital literacy.

5.2.4. To examine the extent to which governments in the Global South are involved in enabling or impeding digital colonialism and surveillance capitalism.

The governments situated in the Global South exert a notable influence in facilitating or obstructing the practise of digital colonialism and surveillance capitalism. Economic interdependencies compel governments to implement policies that provide incentives for foreign entities to extract and exploit data, thereby inadvertently facilitating such practises.

The phenomenon of digital colonialism can be exacerbated by power differentials stemming from past inequities and constrained bargaining leverage. Furthermore, the regulatory capacities of governments may be restricted due to inadequate resources and technical expertise, thereby hindering their efficacy in tackling the issues presented by these phenomena.

Governments located in the Global South have implemented measures to hinder the practises of digital colonialism and surveillance capitalism. Numerous nations have acknowledged the significance of safeguarding data and privacy rights, resulting in the formulation of extensive legislative frameworks.

Frameworks such as the Personal Data Protection Acts, implemented in countries such as Singapore and Malaysia, provide a set of guidelines for the acquisition, utilisation, and disclosure of personal data. The regulations in question curtail data collection and promote individual agency by prioritising consent, transparency, and accountability. As a result, they serve as a barrier to the practise of digital colonialism.

Governments in the Global South have developed national cybersecurity policies with the objective of improving cybersecurity capabilities and promoting consciousness. The aforementioned policies establish a digital milieu that ensures the protection of data privacy and impedes the practise of surveillance capitalism.

Furthermore, the existence of regulations that are specific to certain sectors, such as finance and healthcare, serves as a hindrance to the implementation of these practises. The Financial Services Act and Islamic Financial Services Act in Malaysia are regulatory measures that govern the management and revelation of financial information, thereby safeguarding the confidentiality of the financial sector. The Health Data Protection Act is a legislative proposal aimed at ensuring the protection of health-related personal data in the healthcare industry.

To conclude, governments situated in the Global South encounter a multifaceted terrain when tackling the issues of digital colonialism and surveillance capitalism. The inadvertent facilitation of these practises can be attributed to economic interdependencies and power disparities, while the effectiveness of their regulation is hindered by limited regulatory capacities.

Governments have implemented noteworthy measures to hinder the practises of digital colonialism and surveillance capitalism. By means of the establishment of legislative frameworks, national cybersecurity policies, and regulations tailored to specific sectors, they evince their dedication to safeguarding privacy rights and personal data. Sustained endeavours aimed at enhancing regulatory capabilities and promoting global collaboration are imperative to guarantee fair digital advancement and uphold personal freedoms in developing regions.

5.2.5. To scrutinise the legal and regulatory frameworks of the Global South that facilitate digital colonialism and surveillance capitalism.

The legal and regulatory frameworks of the Global South have a significant impact on facilitating or impeding digital colonialism and surveillance capitalism. While some countries have implemented measures to protect privacy rights and regulate data practises, others have gaps in their legislation that enable exploitative practises. By scrutinising these frameworks, we can gain insight into the specific aspects that contribute to the facilitation of digital colonialism and surveillance capitalism in the Global South.

In some instances, the legal and regulatory frameworks of the Global South facilitate digital colonialism and surveillance capitalism through weak or inadequate privacy laws. Many countries lack comprehensive data protection legislation, leaving individuals vulnerable to data exploitation by both domestic and foreign entities.

The absence of stringent requirements for obtaining consent, limited provisions for data breach notification, and weak enforcement mechanisms create an environment where personal data can be collected, utilised, and disclosed without sufficient safeguards. These loopholes allow for the unchecked accumulation and exploitation of personal data, contributing to the facilitation of digital colonialism.

Additionally, governments in the Global South may adopt policies that prioritise economic development over privacy rights. This can lead to the establishment of data-friendly environments that attract foreign investment but fail to adequately protect individuals' personal data.

Governments often offer incentives and exemptions to multinational corporations, allowing them to operate with fewer restrictions and bypass privacy regulations. These policies may include tax breaks, relaxed data localization requirements, and lenient enforcement mechanisms. By prioritising economic interests over privacy concerns, governments indirectly enable surveillance capitalism and allow foreign entities to exploit personal data without sufficient accountability.

The regulatory frameworks of the Global South also contribute to digital colonialism and surveillance capitalism through limited oversight and regulatory capacities. Many countries lack the resources, technical expertise, and institutional frameworks necessary to effectively regulate the rapidly evolving digital landscape. This results in challenges in monitoring data practises, enforcing privacy laws, and addressing emerging technologies that can infringe on privacy rights.

Insufficient regulatory capacities create an environment where surveillance capitalism can thrive, as companies operate with little fear of repercussions for their data exploitation practises. The lack of regulatory oversight allows foreign entities to exploit personal data without adequate checks and balances, reinforcing power imbalances and perpetuating digital colonialism.

Furthermore, international power dynamics and economic interdependencies can influence the legal and regulatory frameworks of the Global South in ways that facilitate digital colonialism and surveillance capitalism. Historical imbalances and limited negotiating power can lead to unequal trade agreements and partnerships that favour the interests of more powerful nations. These agreements often prioritise the

flow of data and facilitate data extraction from the Global South, exacerbating digital colonialism.

Limited negotiating power can also result in weaker data protection provisions in international agreements, further undermining privacy rights and enabling surveillance capitalism.

However, it is important to note that not all legal and regulatory frameworks in the Global South facilitate digital colonialism and surveillance capitalism. Some countries have recognised the need for robust privacy laws and have implemented comprehensive data protection legislation. These frameworks prioritise individual consent, transparency, and accountability, aiming to protect personal data from exploitation.

Countries like Singapore and Malaysia have enacted Personal Data Protection Acts, establishing guidelines for data collection, utilisation, and disclosure while empowering individuals to exercise their rights. Such frameworks act as a safeguard against digital colonialism and surveillance capitalism, setting a precedent for responsible data practises.

In conclusion, the legal and regulatory frameworks of the Global South have varying degrees of facilitation or impeding influence on digital colonialism and surveillance capitalism. Weak privacy laws, policies that prioritise economic interests over privacy rights, limited regulatory capacities, and international power dynamics contribute to the facilitation of these practises.

However, some countries have taken significant steps to protect privacy rights through comprehensive data protection legislation. Strengthening regulatory capacities, promoting international cooperation, and prioritising privacy rights in policy decisions are crucial steps to impede digital colonialism and surveillance capitalism in the Global South.

5.3. SUGGESTIONS

To address the challenges posed by surveillance capitalism and digital colonialism, comprehensive and ethical strategies are necessary. Safeguarding individual rights, promoting fair competition, and addressing power imbalances created by the dominance of multinational corporations in the digital sphere should be key priorities.

This includes implementing robust data protection regulations, fostering transparency and accountability, and empowering users with greater control over their personal information.

Some additional suggestions for policymakers to address the challenges of data colonialism, surveillance capitalism, and the protection of privacy rights:

1. Implement Data Minimization Principles: Encourage organisations to collect and retain only the minimum amount of personal data necessary for their legitimate purposes. This principle helps reduce the risks associated with data breaches and unauthorised access, and it respects individuals' privacy by limiting the collection and storage of unnecessary information.

2. Establish Privacy-Enhancing Technologies: Promote the development and adoption of privacy-enhancing technologies (PETs) that can help individuals protect their privacy while still benefiting from digital services. Examples include encryption tools, anonymization techniques, and differential privacy mechanisms that safeguard personal data.

3. Enable User Empowerment: Empower individuals with greater control over their personal data through user-centric privacy settings and consent mechanisms. Provide accessible tools that allow users to manage their privacy preferences, easily access and delete their data, and make informed choices about data sharing.

4. Encourage Data Portability: Promote the portability of personal data, enabling individuals to easily transfer their data between different platforms and services. This enhances user autonomy and encourages competition by reducing barriers to switching between providers while ensuring the continued protection of privacy rights.

5. Foster Privacy-Preserving Business Models: Encourage the adoption of business models that prioritise privacy and data protection. Support initiatives that explore alternative revenue models, such as subscription-based services or data trusts, that give individuals greater control over the use of their data and ensure fair value exchange.

6. Enhance Digital Literacy and Education: Invest in educational programmes that promote digital literacy and provide individuals with the knowledge and skills to

protect their privacy rights. This includes teaching individuals about online privacy risks, data protection best practises, and critical evaluation of digital services and platforms.

7. Strengthen Cross-Sector Collaboration: Foster collaboration between governments, industry stakeholders, civil society organisations, and academia to develop comprehensive strategies for data protection and privacy. Engage in multi-stakeholder dialogues and initiatives to ensure diverse perspectives are considered in policy-making processes.

8. Conduct Privacy Impact Assessments: Require organisations to conduct privacy impact assessments (PIAs) before implementing new technologies or data processing practises. PIAs help identify potential privacy risks and develop mitigation strategies, ensuring that privacy considerations are integrated into decision-making processes.

9. Encourage Ethical AI Practises: Promote the responsible and ethical use of artificial intelligence (AI) technologies, particularly in relation to data privacy. Develop guidelines and standards for AI applications that prioritise privacy, transparency, and accountability, and establish mechanisms for auditing and assessing AI systems' impact on privacy rights.

10. Strengthen International Cooperation and Harmonisation: Collaborate with other countries and international organisations to establish harmonised data protection standards and frameworks. This includes sharing best practises, aligning regulations, and developing mechanisms for cross-border data protection and cooperation.

11. Support Independent Auditing and Certification: Encourage independent auditing and certification of organisations' data protection practises. This can help build trust and transparency, allowing individuals to make informed decisions about sharing their data with certified entities that adhere to recognised privacy standards.

12. Ensure Adequate Resources for Data Protection Authorities: Provide sufficient resources, funding, and personnel to data protection authorities to effectively carry out their regulatory and oversight functions. This includes conducting investigations, enforcing compliance, and responding to individuals' privacy complaints in a timely and effective manner.

By implementing these suggestions, governments and policymakers can work towards a digital landscape that respects privacy rights, mitigates the negative impacts of data colonialism and surveillance capitalism, and fosters a more privacy-conscious and user-centric approach to data handling.

BIBLIOGRAPHY

Aaronson SA, 'Data Is a Development Issue' (2019) Centre for International Governance Innovation (CIGI) Papers, No. 223 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3589827> accessed 30 June 2023.

Adepetun A, 'NCC targets consumer protection, infrastructure expansion.' (The Guardian, 13 January 2021) <https://guardian.ng/technology/ncc-targets-consumer-protection-infrastructure-expansion/> accessed 30 June 2023.

Adepetun A, 'NCC targets faster resolution of consumer complaints.' (The Guardian, 29 July 2020) <https://guardian.ng/business-services/ncc-targets-faster-resolution-of-consumer-complaints/> accessed 30 June 2023.

Amazon, 'About Amazon' <https://www.aboutamazon.com/> accessed 30 June 2023.

Amazon Web Services (AWS), 'Cloud computing with AWS.' <https://aws.amazon.com/what-is-aws/> accessed 30 June 2023.

Amnesty Press Release, 'Facebook and Google's pervasive surveillance poses an unprecedented danger to human rights' (Amnesty International, 21 November 2019) <https://www.amnesty.org/en/latest/press-release/2019/11/google-facebook-surveillance-privacy/> accessed 30 June 2023.

Arbab P, 'Global and Globalizing Cities from the Global South: Multiple Realities and Pathways to Form a New Order.' (2019) 18 (3) Perspectives on Global Development and Technology 327.

Arnett C, 'Race, Surveillance, Resistance.' (2020) 81(6) Ohio State Law Journal 1103-1142.

Arora P, 'The Bottom of the Data Pyramid: Big Data and the Global South' (2016) International Journal of Communication vol.10.

Arthur C, 'Microsoft warns of new zero-day flaw targeting Internet Explorer' (The Guardian, 18 September 2012) <https://www.theguardian.com/technology/2012/sep/18/microsoft-internet-explorer-zero-day-flaw> accessed 30 June 2023.

Barrett B, ‘Lawmakers can’t ignore facial recognition’s bias anymore.’ (Wired, 26 July 2018) <https://www.wired.com/story/amazon-facial-recognition-congress-bias-law-enforcement/> accessed 30 June 2023.

Bartz D, ‘Amazon’s Ring used to spy on customers, FTC says in privacy settlement.’ (Reuters, 30 June 2023) <https://www.reuters.com/legal/us-ftc-sues-amazoncoms-ring-2023-05-31/> accessed 30 June 2023.

Beydoun KA, ‘The New State of Surveillance: Societies of Subjugation’ (2022) 79 Wash & Lee L Rev 769.

Birhane A, ‘Algorithmic Colonisation of Africa’ (The Elephant, 21 August 2020) <https://www.theelephant.info/long-reads/2020/08/21/algorithmic-colonisation-of-africa/> accessed 30 June 2023.

Bottis M and Bouchagiar G, ‘Personal Data v. Big Data: Challenges of Commodification of Personal Data’ (2018) 8 Open Journal of Philosophy <https://doi.org/10.4236/ojpp.2018.83015> accessed 30 June 2023.

Brazilian Internet Steering Committee (CGI.br), ‘About the CGI.br’ (CGI.br, 30 June 1995) <https://www.cgi.br/about/#:~:text=The%20Brazilian%20Internet%20Steering%20Committee,well%20as%20promoting%20technical%20quality%2C> accessed 30 June 2023.

Brazilian Internet Steering Committee (CGI.br), ‘CGI.br publishes guidelines and recommendations for the application of Internet laws in Brazil’ (CGI.br Press Release, 31 January 2018) <https://www.cgi.br/noticia/releases/cgi-br-publica-diretrizes-e-recomendacoes-para-aplicacao-de-leis-sobre-internet-no-brasil/> accessed 30 June 2023.

Cadwalladr C and Harrison EG, ‘Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach’ (The Guardian, 17 March 2018) <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election> accessed 30 June 2023.

Central Bank of Nigeria, ‘Consumer Protection Framework Guidelines on Disclosure and Transparency.’ (CBN.gov.ng)

<https://www.cbn.gov.ng/Out/2019/CCD/Draft%20Guidelines%20on%20%20Disclosure%20and%20Transparency%20(002).pdf> accessed on 30 June 2023.

Centre for Information Policy Leadership (CIPL) and Centro de Direito, Internet e Sociedade of Instituto Brasiliense de Direito Público (CEDIS-IDP), 'The Role of the Brazilian Data Protection Authority (ANPD) under Brazil's New Data Protection Law (LGPD)' (CIPL-CEDIS-IDP Joint Project, 17 April 2020).

Cohen JE, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (Oxford University Press 2019).

Coleman D, 'Digital Colonialism: The 21st Century Scramble for Africa through the Extraction and Control of User Data and the Limitations of Data Protection Laws' (2019) 24 Mich J Race & L 417.

Confessore N, 'Cambridge Analytica and Facebook: The Scandal and the Fallout So Far' (The New York Times, 04 April 2018) <https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html> accessed 30 June 2023.

Coppock M, 'France's National Data Protection Commission says Windows 10 collects too much data' (onmsft.com, 20 July 2016) <https://www.onmsft.com/news/frances-national-data-protection-commission-says-windows-10-collects-much-data/> accessed 30 June 2023.

Couldry N and Mejias UA, 'Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject' (2019) Television & New Media, 20(4), 336–349. <https://doi.org/10.1177/1527476418796632> accessed 30 June 2023.

Couldry N and Mejias UA, The Costs of Connection: How Data is Colonising Human Life and Appropriating It for Capitalism (Stanford University Press 2019).

Council for Transparency, 'CPLT questions that SUBTEL asks for personal data of users to telecommunications companies.' (CPLT, 06 August 2020) <https://www.consejotransparencia.cl/cplt-cuestiona-que-subtel-pida-datos-personales-de-usuarios-a-empresas-de-telecomunicaciones/> accessed 30 June 2023.

Criddle C, ‘Facebook sued over Cambridge Analytica data scandal’ (BBC, 28 October 2020) <https://www.bbc.com/news/technology-54722362> accessed 30 June 2023.

DeepMind Technologies Limited, ‘DeepMind’ (2014) <https://www.deepmind.com/> accessed 30 June 2023.

Djik JV, *The Digital Divid*e (Cambridge, Polity Press 2020).

Donnelly C, ‘Xbox Live users hit by data breach.’ (ITPRO, 20 March 2013) <https://www.itpro.com/data-leakage/19470/xbox-live-users-hit-data-breach> accessed 30 June 2023.

Echeverría AA, ‘New bill on cyber security in Chile.’ (Lexology, 20 July 2022) <https://www.lexology.com/library/detail.aspx?g=efc2cfc3-f084-478f-8359-28aba97e1e41> accessed 30 June 2023.

European Data Protection Board (EDPB), ‘€1.2 billion fine for Facebook as a result of EDPB binding decision’ (EDPB, 22 May 2023) <https://edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en> accessed 30 June 2023.

Feiner L, ‘DOJ case against Google likely won’t go to trial until late 2023, judge says.’ (CNBC, 18 December 2020) <https://www.cnbc.com/2020/12/18/doj-case-against-google-likely-wont-go-to-trial-until-late-2023-judge-says.html> accessed 30 June 2023.

Fowler GA and Hunter T, ‘When you “Ask app not to track”, some iPhone apps keep snooping anyway’. (The Washington Post, 23 September 2021) <https://www.washingtonpost.com/technology/2021/09/23/iphone-tracking/> accessed 30 June 2023.

Gatica M and Urzua J, ‘Chile – Data Protection Overview.’ (OneTrust LLC, 30 November 2022) <https://www.dataguidance.com/notes/chile-data-protection-overview> accessed 30 June 2023.

Ghaffary S, ‘Edward Snowden says Facebook is just as untrustworthy as the NSA’ (Vox, 31 October 2019)

<https://www.vox.com/recode/2019/10/31/20940532/edward-snowden-facebook-nsa-whistleblower> accessed 30 June 2023.

Google, 'About Google', (2015) <https://about.google/> accessed 30 June 2023.

Google Policies, 'Privacy Policy' (15 December 2022) <https://policies.google.com/privacy> accessed 30 June 2023.

Greenwald G and MacAskill E, 'NSA Prism program taps in to user data of Apple, Google and others' (The Guardian, 07 June 2013) <https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data> accessed 30 June 2023.

Greenwald G and MacAskill E, 'Obama orders US to draw up overseas target list for cyber-attacks' (The Guardian, 07 June 2013) <https://www.theguardian.com/world/2013/jun/07/obama-china-targets-cyber-overseas> accessed 30 June 2023.

Greenwald G, MacAskill E, Poitras L, Ackerman S and Rushe D, 'Microsoft handed the NSA access to encrypted messages' (The Guardian, 12 July 2013) <https://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data> accessed 30 June 2023.

Greenwood F, 'Data colonialism, surveillance capitalism and drones.' In *Mapping Crisis: Participation, Datafication and Humanitarianism in the Age of Digital Mapping Book* (University of London Press, Institute of Commonwealth Studies,2020).

Giroux HA, 'Totalitarian Paranoia in the Post-Orwellian Surveillance State.' (2015) 29(2) Cultural Studies, Routledge, Taylor and Francis Group.

Harte J, Edwards J and Love J, 'N.Y. judge backs Apple in encryption fight with government' (Reuters, 01 March 2016) <https://www.reuters.com/article/us-apple-encryption-deny-idUSKCN0W22Q0> accessed 30 June 2023.

Harwell D and Dou E, 'Huawei tested AI software that could recognize Uighur minorities and alert police, report says.' (The Washington Post, 8 December 2020) <https://www.washingtonpost.com/technology/2020/12/08/huawei-tested-ai-software-

that-could-recognize-uighur-minorities-alert-police-report-says/> accessed 30 June 2023.

Hashim MSB, ‘Malaysia's National Cyber Security Policy: The country's cyber defence initiatives.’ (2011) Proceedings of the Second Worldwide Cybersecurity Summit (WCS), IEEE Conference Proceeding, London, UK.

Haynes B, ‘Facebook executive jailed in Brazil as court seeks WhatsApp data’ (Reuters, 01 March 2016) <https://www.reuters.com/article/us-facebook-brazil-idUSKCN0W34WF> accessed 30 June 2023.

Heeks R, ‘Digital inequality beyond the digital divide: conceptualizing adverse digital incorporation in the global South’, (2022) Information Technology for Development 28(4) pp. 688-704, DOI: 10.1080/02681102.2022.2068492.

Heiligenstein MX, ‘Microsoft Data Breaches: Full Timeline Through 2023’ (Firewall Times, 06 April 2023) <https://firewalltimes.com/microsoft-data-breach-timeline/> accessed 30 June 2023.

Human Rights Watch, ‘Uganda: Stop Police Harassment of LGBT People.’ (Human Rights Watch, 17 November 2019) <https://www.hrw.org/news/2019/11/17/uganda-stop-police-harassment-lgbt-people> accessed 1 June 2023.

India Brand Equity Foundation, ‘Digital Payments and their impact on the Indian Economy.’ (IBEF.org, April 2022) <https://www.ibef.org/research/case-study/digital-payments-and-their-impact-on-the-indian-economy> accessed 30 June 2023.

International Telecommunication Union (ITU) statistics, ‘Measuring Digital Development: Facts and Figures.’ (2022) <https://www.itu.int/itu-d/reports/statistics/2022/11/24/ff22-internet-use/> accessed 30 June 2023.

Jimenez A and Oleson JC, ‘The Crimes of Digital Capitalism’ (2022) 48 Mitchell Hamline L Rev 971.

Kakar G, ‘Cognitive Dysphoria: Evaluating the Paradigm Shift of Artificial Intelligence Technology in Digital Colonialism’ (2021) 2 Indian J Artificial Intel & L 7.

Kedmey D, ‘Hackers Leak Explicit Photos of More Than 100 Celebrities’ (Time, 01 September 2014) <https://time.com/3246562/hackers-jennifer-lawrence-cloud-data/> accessed 30 June 2023.

Kolade E, ‘Cybersecurity in Nigeria’s Financial Industry: Enhancing Consumer Trust and Security.’ (Carnegie Endowment for International Peace, 13 May 2022) <https://carnegieendowment.org/2022/05/13/cybersecurity-in-nigeria-s-financial-industry-enhancing-consumer-trust-and-security-pub-87123> accessed 30 June 2023.

Kwet M, ‘Digital colonialism: US empire and the New Imperialism in the Global South.’ (2019) Race & Class 60(4) DOI: 10.1177/0306396818823172 <https://ssrn.com/abstract=3232297> accessed 30 June 2023.

Lei Geral de Proteção de Dados Pessoais (LGPD) Law No.13709/2018. <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm> accessed 30 June 2023.

Malwitz CC, ‘Particular Social Groups: Vague Definitions and an Indeterminate Future for Asylum Seekers’ (2018) 83(3) Brooklyn Law Review.

Mann S, ‘Veilance and reciprocal transparency: Surveillance versus sousveillance, AR glass, lifeglogging, and wearable computing’ (2013) IEEE International Symposium on Technology and Society (ISTAS): Social Implications of Wearable Computing and Augmediated Reality in Everyday Life, Toronto, ON, Canada, 2013. DOI:10.1109/ISTAS.2013.6613094.

Marco Civil da Internet (Federal) Law No.12965/2014. <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm> accessed 30 June 2023.

Marker SL, Verstergaard M and Hendricks VF, ‘Digital Colonialism on the African Continent’ (2019) IOL Business Report <https://www.iol.co.za/business-report/opinion/opinion-digital-colonialism-on-the-african-continent-17493010> accessed on 30 June 2023.

Meta Newsroom, ‘Facebook to Acquire Instagram’ (09 April 2012) <https://about.fb.com/news/2012/04/facebook-to-acquire-instagram/> accessed 30 June 2023.

Meta Newsroom, ‘Facebook to Acquire Oculus’ (March 25, 2014) <https://about.fb.com/news/2014/03/facebook-to-acquire-oculus/> accessed 30 June 2023.

Meta Newsroom, ‘Facebook to Acquire WhatsApp’ (February 19, 2014) <https://about.fb.com/news/2014/02/facebook-to-acquire-whatsapp/> accessed 30 June 2023.

Microsoft, ‘About us’ <https://www.microsoft.com/en-us/about> accessed 30 June 2023.

Microsoft Corporation, ‘Microsoft Annual Report 2022.’ (28 July 2022) <https://www.microsoft.com/investor/reports/ar22/ > accessed 30 June 2023.Meta Inc, ‘Company information, Culture and Principles – About Meta’ <https://about.meta.com/company-info/> accessed 30 June 2023.

Mimiko NO, *Globalization: The Politics of Global Economic Relations and International Business* (Durham, North Carolina Academic Press, 2012).

Ministry General Secretariat of the Presidency, ‘Law 19628: On the Protection of Privacy.’ (Promulgation: 18 August 1999, Publication: 28 August 1999, Last Modified: 10 November 2022 – Law 21504)

Ministry General Secretariat of the Presidency, Ministry of Economy, Development, and Tourism, and Ministry of Finance, ‘11144-07 Merged with 11092-07: It regulates the protection and processing of personal data and creates the Agency for the Protection of Personal Data.’ (Honourable Chamber of Deputies of Chile, 15 March 2017) <https://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=11661&prmBoletin=11144-07> accessed 30 June 2023.

Nakashima E, ‘NSA surveillance program still raises privacy concerns years after exposure, member of privacy watchdog says.’ (The Washington Post, 29 June 2021) <https://www.washingtonpost.com/national-security/nsa-surveillance-xkeyscore-privacy/2021/06/29/b2134e7a-d685-11eb-a53a-3b5450fdca7a_story.html> accessed 30 June 2021.

Nakashima R, ‘AP Exclusive: Google tracks your movements, like it or not.’ (Associated Press News, 14 August 2018) <https://apnews.com/article/north-america-science-technology-business-ap-top-news-828aefab64d4411bac257a07c1af0ecb> accessed 30 June 2023.

National Commission for Data Protection Luxembourg, ‘Decision regarding Amazon Europe Core S.à r.l.’ (06 August 2021) <https://cnpd.public.lu/en/actualites/international/2021/08/decision-amazon-2.html> accessed 30 June 2023.

Nwoke U, ‘Access to Information under the Nigerian Freedom of Information Act, 2011: Challenges to Implementation and the Rhetoric of Radical Change.’ (2019) 63(3) Journal of African Law, Cambridge University Press.

Osborne H and Parkinson HJ, ‘Cambridge Analytica scandal: the biggest revelations so far’ (The Guardian, 22 March 2018) <https://www.theguardian.com/uk-news/2018/mar/22/cambridge-analytica-scandal-the-biggest-revelations-so-far> accessed 30 June 2023.

Paco SA, ‘Data Colonialism, the Danger It Poses to India’s Democracy, and the Effectiveness of Data Localization Laws as Resistance.’ (2022) 48 Rutgers Computer & Tech LJ 254.

Personal Data Protection Commission, ‘PDPA Legislation Overview.’ (PDPC Singapore Government Agency) <https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation> accessed 30 June 2023.

Personal Data Protection Commission, ‘PDPC: Advisory Committee’ (PDPC Singapore Government Agency) < https://www.pdpc.gov.sg/Who-We-Are/Advisory-Committee > accessed 30 June 2023.

Personal Data Protection Commission, ‘PDPC: Who we are’ (PDPC Singapore Government Agency) <https://www.pdpc.gov.sg/Who-We-Are> accessed 30 June 2023

PRS Legislative Research, ‘Bill track: Draft Digital Personal Data Protection Bill 2022.’ (PRS India, June 2023) <https://prsindia.org/billtrack/draft-the-digital-personal-data-protection-bill-2022> accessed 30 June 2023.

Republic of South Africa, 'Documents: Acts: Electronic Communications and Transactions Act 25 of 2002.' (South African Government Official Portal) <https://www.gov.za/documents/electronic-communications-and-transactions-act> accessed 30 June 2023.

Republic of South Africa, 'Documents: Acts: Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002.' (South African Government Official Portal) <https://www.gov.za/documents/regulation-interception-communications-and-provision-communication-related-information--13> accessed 30 June 2023.

Republic of South Africa, 'Documents: Notices: National Cybersecurity Policy Framework.' (South African Government Official Portal, 04 December 2015) <https://www.gov.za/documents/national-cybersecurity-policy-framework-4-dec-2015-0000> accessed 30 June 2023.

Reuters, 'Amazon hit with record EU data privacy fine.' (Reuters, 30 July 2021) <https://www.reuters.com/business/retail-consumer/amazon-hit-with-886-million-eu-data-privacy-fine-2021-07-30/> accessed 30 June 2023.

Reuters, 'FCC probes Google's Street View data collection' (Reuters, 11 November 2010) <https://www.reuters.com/article/google-privacy-idCNN1021543120101110> accessed 30 June 2023.

Reuters, 'France orders Microsoft to stop collecting excessive user data' (Reuters, 21 July 2016) <https://www.theguardian.com/technology/2016/jul/20/france-microsoft-user-data-collection-privacy> accessed 30 June 2016.

Reuters Staff, 'Facebook agrees to pay UK fine over Cambridge Analytica scandal' (Reuters, 30 October 2019) <https://www.reuters.com/article/us-facebook-privacy-britain-idCAKBN1X913O> accessed 30 June 2023.

Roberts SR, *The War on the Uyghurs: China's Internal Campaign against a Muslim Minority* (Princeton University Press 2020).

Sahbaz U, 'Artificial Intelligence and the Risk of New Colonialism' (2019) Horizons: Journal of International Relations and Sustainable Development, No. 14, The

Importance of being earnest: Geopolitics of Realism (Summer 2019), pp. 58-71, Center for International Relations and Sustainable Development.

Schiller H, *Communication and Cultural Domination* (International Arts and Sciences Press 1976).

Schmidt DC, 'Digital Content Next: Google Data Collection Paper' (21 August 2018) <https://digitalcontentnext.org/wp-content/uploads/2018/08/DCN-Google-Data-Collection-Paper.pdf> accessed 30 June 2023.

Sherif AE, 'The Egyptian Muslim Brotherhood's Failures' (Carnegie Endowment for International Peace, 01 July 2014) <https://carnegieendowment.org/2014/07/01/egyptian-muslim-brotherhood-s-failures-pub-56046> accessed 30 June 2023.

Singh P, 'Aadhaar and data privacy: biometric identification and anxieties of recognition in India.' (2019) 24 (3) Information, Communication & Society.

Skelton M, 'What the Apple versus FBI Debacle Taught Us' (Scientific American, 20 May 2016) <https://blogs.scientificamerican.com/guest-blog/what-the-apple-versus-fbi-debacle-taught-us/> accessed 30 June 2023.

StatCounter Global Stats, 'Search Engine Market Share Worldwide' (May 2023) <https://gs.statcounter.com/search-engine-market-share> accessed 30 June 2023.

Statista Research Department, 'Apple's global brand value from 2006 to 2022.' (Statista, 03 April 2023) <https://www.statista.com/statistics/326052/apple-brand-value/> accessed 30 June 2023.

Statista Research Department, 'Annual net sales revenue of Amazon from 2004 to 2022.' (Statista, 14 February 2023) <https://www.statista.com/statistics/266282/annual-net-reenue-of-amazoncom/> accessed 30 June 2023.

Statista Research Department, 'Microsoft's global brand value from 2006 to 2022.' (Statista, 06 January 2023) <https://www.statista.com/statistics/326058/microsoft-brand-value/> accessed 30 June 2023.

Sulkowski AJ, Hartigan DB, Goldberg CB, Verbos AK, Bu ML and Nunez RMB, 'Systems Theory, Surveillance Capitalism, and Law: Native Wisdom and Feedback Loops to Boost the Constructive Use of Big Data' (2022) 20 Colo Tech LJ 121.

Swales L, 'The Protection of Personal Information Act and data de-identification Discussions on POPIA'. (2021) 117(7/8) South African Journal of Science.

Tanfani J, 'Race to unlock San Bernardino shooter's iPhone was delayed by poor FBI communication, report finds' (Los Angeles Times, 27 March 2018) <https://www.latimes.com/politics/la-na-pol-fbi-iphone-san-bernardino-20180327-story.html> accessed 30 June 2023.

Thatcher JE and Dalton CM, 'What are our data, and what are they worth?' (2022) Data Power: Radical Geographies of Control and Resistance, pp.46–64. Pluto Press. <https://doi.org/10.2307/j.ctv249sg9w.9.> accessed 30 June 2023.

Therien JP, 'Beyond the North-South divide: The two tales of world poverty.' (1999) 20 (4) Third World Quarterly 723.

The Guardian, 'The Snowden files' (The Guardian, 12 February 2017) <https://www.theguardian.com/world/series/the-snowden-files> accessed 30 June 2023.

The InfoComm Media Development Authority (IMDA) and Personal Data Protection Commission (PDPC), 'Enabling Data-Driven Innovation Through Trusted Data Sharing in a Digital Economy.' (IMDA Singapore Government Agency, 28 June 2019) <https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/archived/imda/press-releases/2019/enabling-data-driven-innovation-through-trusted-data-sharing-in-a-digital-economy> accessed 30 June 2023.

The InfoComm Media Development Authority (IMDA), 'Official Launch of Data Protection Trustmark' (IMDA Singapore Government Agency, 09 January 2019) <https://www.imda.gov.sg/-/media/Imda/Files/Programme/DPTM/DPTM-Information-Kit.pdf > accessed 30 June 2023.

The Organization for Economic Cooperation and Development (OECD), 'Agreement on the terms of accession of the Republic of Chile to the Convention on the

Organisation for Economic Co-operation and Development.' (OECD.org, 11 January 2010) <https://www.oecd.org/chile/44381035.pdf> accessed 30 June 2023.

Toor A, 'France orders Microsoft to stop tracking Windows 10 users' (The Verge, 21 July 2016) <https://www.theverge.com/2016/7/21/12246266/france-microsoft-privacy-windows-10-cnil> accessed 30 June 2023.

United Nations Department of Economic and Social Affairs (UN-DESA), 'World Social Report 2020: Inequality in a rapidly changing world.' (2020) <https://www.un.org/development/desa/dspd/wp-content/uploads/sites/22/2020/02/World-Social-Report2020-FullReport.pdf> accessed on 1 June 2023.

United States Securities and Exchange Commission, 'Apple Inc. Fiscal 2022 Annual Report (Form 10-K)' (28 October 2022) <https://www.sec.gov/ix?doc=/Archives/edgar/data/320193/000032019322000108/aapl-20220924.htm> accessed 30 June 2023.

United States Securities and Exchange Commission, 'Form 8-K: Current Report Pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934' (2015) <https://www.sec.gov/Archives/edgar/data/1652044/000119312515336577/d82837d8k12b.htm> accessed 30 June 2023.

Verily Life Sciences LLC, 'Verily: Home' (2015) <https://verily.com/> accessed 30 June 2023.

Viljoen S, 'A Relational Theory of Data Governance' (2021) 131 Yale L J 573.

Waymo, 'Waymo – Autonomous Driving Technology Company' (2016) <https://waymo.com/> accessed 30 June 2023.

Wheeler T, Verveer P, and Kimmelman G, 'The need for regulation of big tech beyond antitrust' (Brookings, 23 September 2020) <https://www.brookings.edu/blog/techtank/2020/09/23/the-need-for-regulation-of-big-tech-beyond-antitrust/> accessed 1 June 2023.

Winder D, 'Microsoft Security Shocker As 250 million Customer Records Exposed Online' (Forbes, 22 January 2020) <https://www.forbes.com/sites/daveywinder/2020/01/22/microsoft-security-shocker-

as-250-million-customer-records-exposed-online/?sh=25f9bdb54d1b> accessed 30 June 2023.

Wong JC, ‘Facebook to be fined $5bn for Cambridge Analytica privacy violations – reports’ (The Guardian, 12 July 2019) <https://www.theguardian.com/technology/2019/jul/12/facebook-fine-ftc-privacy-violations> accessed 30 June 2023.

Wong JC, Lewis P and Davies H, ‘How academic at centre of Facebook scandal tried and failed to spin personal data into gold’ (The Guardian, 24 April 2018) <https://www.theguardian.com/news/2018/apr/24/aleksandr-kogan-cambridge-analytica-facebook-data-business-ventures> accessed 30 June 2023.

World Population Review, ‘Global South Countries: A Complete List.’ (2023) <https://worldpopulationreview.com/country-rankings/global-south-countries> accessed 30 June 2023.

Yadron D, ‘FBI confirms it won’t tell Apple how it hacked San Bernardino shooter’s iPhone’ (The Guardian, 28 April 2016) <https://www.theguardian.com/technology/2016/apr/27/fbi-apple-iphone-secret-hack-san-bernardino> accessed 30 June 2023.

Zuboff S, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile Books England 2019).