Assessing Legal Responsibilities and Accountability Mechanisms of Big Data Companies Through the European Convention on Human Rights (ECHR)

Research Dissertation Presented in Partial Fulfilment of the Requirements for the Degree of LLM in International Human Rights Law (QQI)

Law School, Griffith College, Dublin

Mark Anthony Achonu-Douglasson

2023/2024

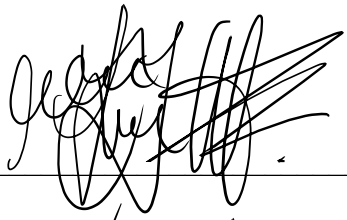
Candidate Declaration

Candidate Name: **Mark Anthony Achonu-Douglasson**

I certify that the dissertation is entitled: **Assessing Legal Responsibilities and Accountability Mechanism of Big Data Companies Through the European Convention on Human Rights.**

Submitted for the degree of: **Master of Laws in International Human Rights Law**

Is the result of my own work and that where reference is made to the work of others, due acknowledgement is given.

Candidate Signature: 

Date: August 9th, 2024

Supervisor Name: **Caoimhe Kiernan**

Signature: _____

Date: _____

Dedication

To my ‘Fantastic Four’, **Thandeka, John Paul, Faith and Wilberforce** whose love and patience with me allowed me the time to further my education.

Table of Contents **Page**

LIST OF ABREVIATION

LIST OF ABREVIATION

CLS	Critical Legal Studies
CoE	Council of Europe
CFR	Charter of Fundamental Rights of the European Union
DPA	Data Protection Authority
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
GA	General Advocate
GDPR	General Data Protection Regulation
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
ECJ	European Court of Justice
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EU	European Union
IOT	Internet of Things
TNC	Transnational Corporation
UDHR	Universal Declaration of Human Rights
UN	United Nations
VR	Virtual Reality

Abstract

The increasing expansion of big data companies and technologies have raised concerns about the protection of the right to privacy, data protection and the principle of non-discrimination. 'Datafication' through collecting, storing and processing of massive amount of personal data raise questions of legal obligations and accountability. This study examines the role of the European Convention on Human Rights (ECHR) in addressing these concerns through ethical practices that protects individual rights in this digital era.

This study made a comprehensive analysis of the ECHR's provisions that is key to the operations of big data companies. It focused on Article 8 (the right to respect for private and family life) or the right to privacy, Article 10 (freedom of expression) and Article 13 (right to remedy) in relation to emerging issues of the datafication of the society. This thesis evaluated the impact of these rights on big data activities using doctrinal and socio-legal methodology in scrutinizing the ECHR and case law from ECtHR principles applicable to the digital age.

This study identified the gaps and challenges in regulating the big data operation through the ECHR, while proposing a balanced approach between data analytical process and human rights. This study investigated the ECHR regulatory frameworks including the GDPR on enforcement efficacy and standards. It assessed the role of European and national data protection authorities and cross border collaborations for accountability mechanism.

This study argued that the ECHR remains a relevant framework in the regulation of data protection but requires adaptation to effectively address the challenges posed by the pace of emerging technological innovations by integrating the principles of transparency, accountability and fairness. The ECHR can enhance legal responsibility and accountability mechanisms through ethically driven practices by big data companies as a catalyst for safeguarding the right to privacy and data protection. The findings contribute to the current discourse on privacy rights, data protection and offering insights for policy makers, regulators and big data companies.

Keywords: Big Data, ECHR, ECtHR, Legal Responsibilities, Accountability Mechanisms, Data Protection, GDPR, Human Rights, Digital Rights, Regulatory Frameworks.

CHAPTER ONE

1. Introduction

1.1. Background

Big data plays a crucial role in the global economic system and has overtaken oil as the new engine of growth and development.[1] While its open new opportunities to the society, it is not without challenges. This research will focus on investigating the relationship between big data companies and human rights by focusing on assessing the legal responsibilities and accountability mechanisms under the European Convention on Human Rights (ECHR). Current advances in big data, artificial intelligence, and data-driven innovation have positive outcomes but could unleash mayhem if these are mismanaged.[2] Unethical practices could lead to the data process bypassing the original intent of ensuring that the rights to privacy and individual data are protected.[3]

This major challenge of big data must be solved as our society is fast moving towards a process of 'datafication' where devices have the capacity to capture, collect, store and process data in a cheaper, better and faster way.[4] The speed and urgency in the evolution of technology with the widespread collection of data, processing, and use of data by big data companies is a global concern especially on the potential implications with human rights.

While sensitive data are entrusted to big data companies daily, there has been increasing cases of data leakage, hacking and breach of individual privacy rights and personal security of the users.[5] Increasing role of big data companies in the world has geopolitical implications, when one looks at how these companies' operations transcend borders and dominates people's opinions and choices.[6] Non-state actors with extraterritorial and jurisdictional powers could continue to violate people's fundamental human rights in environment, labour, immigration, and freedom of speech

[1] Nersessian, David 'The law and ethics of big data analytics: A new role for international human rights in the search for global standards' (Business Horizons, 61 no 6 2018) p 845-854.
[2] Bormida, Marina Da 'The big data world: Benefits, threats and ethical challenges' In *Ethical Issues in Covert, Security and Surveillance Research* (Emerald Publishing Limited 2021) p 71-91.
[3] Ibid.
[4] Ibid.
[5] Ibid.
[6] Johansen, Stian Oby '*The human rights accountability mechanisms of international organizations*' (Cambridge University Press, 2020).

without the proper legal framework and mechanisms to promote and protect them.[7] With the slow bureaucratic nature of states operations and governance, in response to the rate of rapid developments and changes in the field of data usage and management, it becomes an imperative to examine the legal responsibilities and accountability mechanisms that controls their operations.

The need to respect human rights was evidenced in the adoption of the United Nations Guiding Principles (UNGP's) as an instrument for a human rights approach for business activities in transnational fields such as big data companies. But the implementational process has been ineffective. Corporate business responsibility is crucial in respecting human rights. However, without active and effective legal mechanisms and framework, they will remain a dreaming.

This study seeks to investigate how far the European Convention on Human Rights (ECHR) has gone as a legal framework for assessment and assurance of legal responsibilities and accountability mechanisms.

1.2. Central Research Question

The purpose of this thesis is to investigate the existing legal obligations of data controllers, especially the big data companies within the context of the European Convention on Human Rights. As the pace of big data technological growth is faster than the rate of legal regulations to ensure the protection of the right to privacy and the right to the protection of personal data. This research will examine the existent norms and identify the gaps and challenges of accountability for human rights violations and will address the following research question:

Central question:

What legal responsibilities do big data companies have on individual privacy rights?

Big data companies are obligated to ensure that data process do not breach the right to privacy. This includes other obligations under the ECHR, such as the right to freedom of expression (Article 10), and Article 13 for effective remedies when any of the provisions is breached.

[7] Michalowski R.J and Kramer R.C. 'The Space Between Laws: The Problem of Corporate Crime in a Transnational Context' Social Problems (Oxford University Press, 1987) 34 (1) p 34 – 36.

Questions following the central research question.

1. How should ECHR be useful in the enforcement of these individual privacy rights?

   Article 8 ensures that the right to private and family life is protected from arbitrary interference by any other public authorities. Also, the European Court of Human Rights comes to the rescue, when national legal remedies are exhausted and failed to redress any violation.

2. What accountability mechanisms can be used to enforce compliance under the ECHR framework?

   A mix of accountability mechanisms including legal, regulatory and independent company policies are important in enforcing compliance. National courts and ECtHR mechanism ensure that unbiased, fair and effective legal procedures are followed.

3. How do ECHR principles such as Article 6, Article 8 and Article 10 apply to big data companies processing personal data?

Under the ECHR, the right to privacy (Article 8) and the right to a fair trial (Article 6) ensure that data process is fair, lawful and transparent. Big data companies must ensure that their activities balance the business needs and human rights of individuals.

1.3. Research Aims and Objectives

To answer the primary research questions, I have identified four specific research objectives as follows:

1.3.1. To identify the problems and gaps in the existing legal frameworks for holding human rights violators accountable. *This involves evaluating the existing laws, regulations and procedure related to human rights violations.*

1.3.2. To analyse the current legal obligations under the ECHR.
The ECHR is crucial in protecting human rights across Europe, and review keys provisions relevant in understanding legal obligations it imposes on data controllers especially the big data companies.

1.3.3. To assess the efficacy and application of the current accountability mechanisms under the ECHR. *This will evaluate how the existing mechanism address privacy rights.*

1.3.4. To offer recommendations to strengthen the legal and accountability mechanisms. *This will follow the analysis, to propose recommendations that might involve reforms or enhanced cooperation among big data stakeholders.*

1.4. Methodologies and Reasons

For the aims of this thesis, there, different research methods could be used for analytical purposes.

Doctrinal methodology is vital to look at the legal texts, cases and statues that established the existing legal framework and mechanisms of the ECHR, which helps in making critical legal reasoning to examine key principles of the established laws such as Article 6, Article 8, and Article 10 for appropriate analysis, insights and recommendations. Critical legal studies (CLS) theory challenges existing legal norms of policy and practice and views the interconnection of law and social issues with its inherent biases.[8] The ECHR legal framework reflects the existing legal and political contexts of states' priorities when it comes to big data companies Economic Value v Human Rights violations, which supports their interests. Also, socio-legal research methodology is an interdisciplinary approach is vital in assessing and examining the intersection of law and the broader social contexts it will sum up the theoretical and empirical analysis through a combination of the perspectives and methodologies from legal and social sciences.[9] This revelation of the law in policy and practise by casting light to the related or alternative realities that shape the society and allowing different legal, political, and social perspective which could provide more insights for analysis and solutions. Socio-legal research key aspects will emphasis on the interdisciplinary nature of this research, make empirical focus with specific key areas of the study.

After a careful review on these research methodologies; I will depend more on the Socio-legal research methodology for a broader, interdisciplinary, and contextual purposes. In applying the social legal research methodology in assessing legal responsibilities and accountability mechanism on big data companies within the framework of the ECHR will help in understanding the legal

[8] Peter Fitzpatrick and Hunt Alan 'Introduction" Journal of Law and Society' [1987] 14(1) p 1 JSTOR > https://doi.org/10.2307/1410292 > (Accessed 18 November 2023).
[9] Johansen, Stian Oby '*The human rights accountability mechanisms of international organizations*' Cambridge (University Press, 2020).

responsibilities, identifying accountability mechanisms and ECHR perspectives and qualitative research method for more insights in understanding how big data companies go through legal responsibilities to make contributions to accountability under human rights contexts of the ECHR.

Both qualitative and quantitative research methods will be used. Qualitative – will include case studies and legal documents and reviews. Selected cases under the ECHR to draw reasonable conclusions and comparisons. Quantitative – human rights violations and statistical analysis.

Data collection - primary data on reviews, court decisions and reports. Secondary data collection policy papers, academic reports and corporate social responsibility reports and books.

1.5. Existing Academic Literature

This research will examine the current literature on legal responsibilities of the big data companies and accountability mechanisms governing within the context of the ECHR and exploring case studies, reviews, and reports for legal insights. The age of big data is commonly known for the collecting and analyzing vast proportion of personal information by companies.[10] This development has brought up concerns on the protection of individuals' rights and privacy. One of the potential frameworks for assessing the legal responsibilities and accountability mechanisms of big data companies is the European Convention on Human Rights.[11] Obviously, the importance and power of big data companies are undeniable and their political effects are felt by states, although, they are not political entities. Also, their economic powers can be equalled or more than many sovereign states today A typical example is Google, while it is not a country, but its data sovereignty in securing its networks resembles that of a normal political state with obligations to uphold rights and responsibilities. [12] Google's CEO's slip of tongue seems to fit into the role of big data companies in 'Netizens' lives these days.[13]

While companies are not sovereign states but are really exercising some of the characteristics of sovereign states such as jurisdictional and extraterritorial influence which are within the

[10] Butin, Denis, and Daniel Le Metayer 'A guide to end-to-end privacy accountability' In *2015 IEEE/ACM 1st International Workshop on Technical and Legal aspects of data privacy and Security* (IEEE, 2015) p 20-25.
[11] Maghfirah, Fitri, and Fathayatul Husna 'CYBER CRIME AND PRIVACY RIGHT VIOLATION CASES OF ONLINE LOANS IN INDONESIA' In *PROCEEDINGS: Dirundeng International Conference on Islamic Studies* (2021) p 1-18.
[12] Anastasiia Zlobina 'Human Rights Obligations of Information and Communication Technology Companies in the Context of Data Governance' [Dissertation] University of Nottingham A.Y. (2017/2018) p 5.
[13] Ibid.

framework and obligations of states.[14] The pace at which big data companies have expanded their operations globally especially where from places with different jurisdictional legal frameworks for accountability and mechanisms appropriate for responsibility and accountabilities is concerning and a recipe for possible breach of human rights.[15] This comparative disadvantage exposes people to vulnerable situations where their data and privacy could be violated. If big data companies have been involved in the increasing cases of breach of privacy and data protection issues in developed states, it indicates troubling evidence of the under reported and unreported issues of breaches in developing states. This problem is one of the reason this research will assess the available legal mechanism within the framework of the European Convention on Human Rights for the operations of big data companies.

Experts have noted a 'corporate veil,' [16] where transnational corporations (TNCs) hide to avoid accountability of human rights violations. They benefit from legal protection due to their legal personality which grants them rights as the evade responsibilities.[17] Also, they have the capacity of interfering with extensive range of human rights, but the existing international law has mostly failed in the provision of mandated duties of these companies and effective framework to hold them accountable for breach of human rights.[18] After the World War II, there was states became the sole subjects of international law with the capacity of obligations for rights and duties. The post-1945 expansion of these international legal roles to people within the context of human rights law and responsibilities could not be extended to TNC's such as big data companies, as international law failed to view them as *'bearers of legal obligations under international criminal law'*.[19] This research will analyse the problems and gaps and evaluate the current legal framework of the ECHR for recommendations.

The ECHR provides a comprehensive legal framework for assessing the legal responsibilities and accountability mechanisms of big data companies.[20] Also, it provides certain rights and freedoms

[14] Ibid.
[15] Michalowski R.J and Kramer R.C (n 7) 34 -36.
[16] Ibid.
[17] Meeran R. 'The Unveiling of Transnational Corporations: A Direct Approach' in Addo M.K. (ed) 'Human Rights Standards and the Responsibility of Transnational Corporation' (The Hague: Kluwer Law International 1999) p 161 – 170.
[18] Harvard Law Review 'Developments in the Law – Criminal Law Part V: Corporate Liability for Violations of International Human Rights Law' (Vol 114 No 7 2001) p 2030 – 2031.
[19] Ibid.
[20] Butin, Denis, and Daniel Le Metayer (n 10).

for individuals which includes the right to privacy and the right to a fair trial. Under the ECHR, data controllers such as the big data companies have a legal responsibility to ensure the security of consumers' data. And must secure informed consent from users and be transparent in their data management processes. Additionally, the European Convention on Human Rights emphasizes the importance of accountability mechanisms for ensuring that individuals' rights are protected.[21] This aspect is significant to finding how the European Convention on Human Rights could be useful in the enforcement of individual privacy rights.

The right to explanation and the right to contest automated decisions are essential part of the mechanisms, which is within the onus of member States to set up safeguards that would guarantee the rights and freedoms of data subjects. Following the obligations as stated under the European Convention on Human Rights, big data companies could fulfill their legal responsibilities in protecting individuals' privacy rights and ensuring accountability for their data processing activities. One potential aspect of legal responsibilities and accountability mechanisms for big data companies is the implementation of laws and regulations, such as the General Data Protection Regulation in the European Union.[22] The General Data Protection Regulation enforces data protection laws and regulations within the European Union, which establishes the legal responsibilities and accountability mechanisms for big data companies operating within the its jurisdiction. And include the right to explanation and ensures that individuals have the right not to be subject to automated decision-making without human role and the possibility to contest and challenge any of the algorithmic decisions. Consequently, these accountability mechanisms can be used to enforce compliance under the ECHR framework.

Member States considered the Article 22 of the General Data Protection Regulation for enabling positive outcomes, as decisions which are based solely on automated processing and do not require human intervention. But the extent to which these positive decisions are allowed under Article 22 is still contentious among the member states. Therefore, big data companies have a legal responsibility to protect consumers' data and adhere to regulations such as the General Data Protection Regulation. And through the European Convention on Human Rights, big data

[21] Gianclaudio Malgieri 'Automated decision-making in the EU Member States: The right to explanation and other "suitable safeguards" in the national legislations' Computer Law & Security Review (Volume 35, Issue 5, 2019) 105327, ISSN 0267-3649 https://doi.org/10.1016/j.clsr.2019.05.002.
[22] GDPR 'REGULATION' (EU) 2016/679.

companies are accountable for ensuring that individuals' rights are protected in relation to their data processing activities. Apparently, there are corporate ‘spider webs’ of financial mobility, extraterritoriality and competitions limit regulatory measures for Tran-National Corporations.[23] The Universal Declaration of Human Rights (UDHR) Article 1[24] and ECHR Article 1 asserts the obligations to uphold and respect human rights and the right to the freedom of expression of Article 10.[25] According to the ‘space between the laws’ which are jurisdictional gaps the violators use to evade justice.[26] It has become obvious that some companies take advantage of the legal differences between their home and host countries and its gap in setting a comprehensible and effective mechanisms of accountability, to perpetuate human rights abuse while performing the normal business operations. Several attempts by the United Nations in developing acceptable codes of conduct for corporate business responsibility have not been effective.

The right to privacy as interpreted in the personal data protection within the General Data Protections Regulations (GDPR) falls within the international human rights scope which the European Court of Human Rights (ECtHR) follows under its right to data privacy of the Article 8 of the ECHR. The failure of political compromise on states for data privacy and protection led to the European data protection framework and regulation through the GDPR. While the ECHR does not contain comprehensive legal codes on data protection, it guarantees these rights through the right to respect private and family life under the scope of the Article 8.[27] As evidenced in the case, S. and Marper v. The United Kingdom [2008] 30562/04 and 30566/04, the courts decision that ‘mere storing of data relating to private life of an individual amounts to an interference within the meaning of Article 8’.[28]

The UDHR, ECHR and GDPR could be instrumental in setting a standard for the promotion and protection of human rights against the errors of data processing by data controllers. Because the increasing global corporate powers raise questions on matching their operations with human rights

[23] Ibid.
[24] UN General Assembly Universal Declaration of Human Rights (UDHR) (1948 217 A III) > Accessed 10 November 2023.
[25] European Convention on Human Rights (ECHR) Article 1 and 10 > Accessed https://www.echr.coe.int/documents/d/echr/guide_art_10_eng > (8 November 2023).
[26] Khoury S. Transnational corporations and the European Court of Human Rights: Reflexions on the Indirect and Direct Approaches to Accountability. Sortuz: (Oñati Journal of Emergent Socio-Legal Studies (2010) 4(1) p 69.
[27] ECHR Art 8.
[28] S. and Marper v. The United Kingdom [2008] 30562/04 and 30566/04 para 67

standards.[29] It remains the responsibility of member states to use and apply the appropriate legal framework within their authority and authority to uphold their legal obligatory responsibilities.[30]

This research will assess the current gaps in the ECHR and identity areas that needs strengthening for legal responsibilities and accountabilities. And the Big data companies have a legal responsibility to protect consumers' data and adhere to regulations such as the General Data Protection Regulation.[31] Through the ECHR, they are held accountable for respecting individuals' rights and freedoms, including the right to explanation and the right to contest and challenge algorithmic decisions. Through this practice the ECHR principles would effectively control the big data companies and other data processors handling personal data. While it is the obligation of states to uphold the ECHR provisions, the courts cases shows the obligations to be followed by data processing companies and the rights to be protected by the state. [32] This research will find answers to the questions of big data companies' rights in data protection among the other data processors such as the government. And how the ECHR would be useful in the enforcement of individual privacy rights.

1.6. Contribution to Existing Knowledge

This research will contribute to the existing body of knowledge in big data companies' legal responsibilities and accountability mechanisms by giving more insights for legal practitioners, policy makers and organizations promoting human rights and better business practices.

1.7. Scope and Limitations

This study's purpose is to assess the legal responsibilities and accountability mechanism of big data companies through the lens of the ECHR. The scope assess the big data companies, their activities and their impact on human rights, especially the rights to privacy and data protection.

The limitations specifically focuses on big data companies, excluding other types of organizations. Secondly, this thesis will use the ECHR framework to analyze accountability mechanisms, with

[29] Ibid 69.
[30] Steiner H.J. et al International Human Rights in Context: Law, Politics, Morals (3rd ed Oxford University Press 2008) p 1388.
[31] Gianclaudio Malgieri (n 21).
[32] Zlobina (n 12) 14.

little emphasis on the General Data Protection Regulation (GDPR), due to its relevance within the EU data protection agenda.

Thirdly, human rights aspects will be explored, going beyond the rights to privacy. Considering the rights to freedom of expression, non-discrimination and redress.

Lastly, this thesis acknowledges the difficulties in investigating big data companies because of their independence and lack of transparency in an evolving digital era.

1.8. Expected Findings

The research will find valuable insights on the legal responsibilities and accountability mechanisms on governing the operations of big data companies under the framework of the European Convention on Human Rights. And contributing to the existing body of knowledge through a comprehensive analysis on the legal responsibilities and accountability mechanisms on data companies, human rights, and the ECHR context.

The findings of this research will be used in furthering academic discourse in fostering corporate accountability and responsibility on human rights issues for global data business operations. Informing policy makers, stakeholders and legal practitioners on the threats and opportunities of proportionality between the protection of human rights and advancement of technology.

1.9. Outline of the Next Chapters

Chapter Two presents the theoretical framework on big data, its nature, applications, and implications according to different terms of the evolution of the data. And evaluates the 'datafication' of the society and the application and implications of big data, with the ethical, and legal aspects for privacy and data protection.

Chapter Three will explore the key principles of the ECHR, obligations and accountability on big data companies. The relationship between the privacy rights, the scope of the freedom of expressions and the right to effective remedy were elaborated. The role and authority of regulatory bodies as centers of the European regulatory centers for the protection of the right to privacy within Europe.

Chapter Four evaluates legal challenges and the interaction between technology and human rights. And will emphasize the development of a balanced approach between technological innovations and human rights. This makes it important to consider the future challenges and directions related to the emerging technologies. This chapter identified the main legal issues with the regulatory authorities, courts and other mechanisms. And the legal gaps that needs to be closed to mitigate the negative impacts of emerging technologies.

Chapter Five will examine the scope of the legal framework regime and its efficacy through the summary of the key findings of the previous chapters, the contributions and recommendations for further studies.

CHAPTER TWO

2.1. Introduction

'Big data' has become a transformative force in our societies and times, which is continuously shaping the way we approach and use information in decision making and business innovation. An increasing number of the society is learning how to live and survive in the digital space that is becoming drown in what seems like a 'sea of data'. This development comes with new realities of opportunities and challenges for both data controllers and data subjects. An appropriate and effective use of data will be of great benefit to the society and undoubtably contribute to the creative and innovative transformation of almost every part of human life. However, the abuse of the intent of data privacy and data protection could lead to an unintended consequence. Especially, now that it has become easier, faster and cheaper to collect, store, process and use data with the advanced by big data technologies for different purposes that bypass the intent of data privacy. This not only poses a risk but is a breach of one of the fundamental principles of human rights.

Ethical use of data by big data companies is not only important, but one of the key obligations of data controllers such as big data companies as enshrined in the European Convention on Human Rights (ECHR), the General Data Protection Regulation (GDPR) and the Universal Declaration of Human Rights (UDHR). Companies are responsible on for data process activities and to ensure public confidence for the personal data with its voluminous development as it gets faster, and bigger and deal with data in different forms, whether structured or unstructured which is a phenomenon known as the 'big data'.[33]

This chapter aims to present the theoretical framework that delves into the definition of big data, its nature, applications and implications according to different terms of the evolution of the data. And the 'datafication' of the society due to the 'data paradigm' that influences behavioral changes for optimum and personalized alternatives. It goes further with the application and implications of big data, with the ethical, and legal aspects for privacy and data protection. This chapter will explore who big data impacts human rights, such as the right to privacy and the right to data protection.

[33] Ishikiriyama, Célia Satiko and Carlos Francisco Simões Gomes 'Big Data: A Global Overview' (Studies in Big Data 2018).

2.2. The Overview of Big Data

Recently, big data has been gaining traction and importance while considering its exponential growth in volume, velocity and variety as it is being generated from different domains.[34] This data explosion is a result of the proliferation of connected digital technologies and devices and increasing digitization of daily human activities.[35] With this development, and 'datafication' of the society, it has become a key priority and drive to generate important insights vital for decision making purposes which could give policy makers, businesses, researchers, and governments the edge in their different engagements. This development poses a threat and the same time an opportunity for businesses, organizations, people and regions such as the European union to find better ways of using and the increasing amount of data for economic development and keeping the protecting the privacy rights of the people. [36]

It is an imperative to make sure that data process will follow ethics and norms that upholds the fundamental principles of human rights to avoid the 'creep factor' of Big Data, which could lead to the flow of data that bypasses the original purpose of privacy and data protection law.[37] An ethically compliant data process that prioritizes society's needs will play a significant role in fostering sustainable development.[38] In making sure that there are reduced impacts on the people's privacy which could be manipulated through high tech profiling, using automated decision making in public services, and applying discriminatory practices that stigmatizes a certain group of people. If such a creepy factor in big data is not identified, observed and corrected, it would lead to a manipulated value system based on pre-programed objectives which might be a breach of privacy rights and create a vulnerable situation. This makes it important to ensure that fairness and accuracy are used in such scoring systems that make important decisions for the society.[39]

[34] Manyika, James, Michael Chui, Brad Brown, Jacques Bughin, Richard Dobbs, Charles Roxburgh, and Angela Hung Byers 'Big data: The next frontier for innovation, competition, and productivity' (2011).
[35] Manyika et al. (n 34).
[36] European Economic and Social Committee 'The ethics of big data: balancing economic benefits and ethical questions of big data in the EU policy context' (*European Union* 2017) p 36.
[37] Bormida, Marina Da (n 2) 71-91
[38] Ibid.
[39] Ibid.

2.3. The Definition and Characteristics of Big Data

In 2020, user generated data grew at the rate of 2000% globally from diverse range of sources.[40] In defining data, it is important to note that there is varied definitions based on the purpose and use. A common feature of all definitions is the reference to a large amount of data that is beyond the analytical capacity of a single computer, but coming from diverse sources, and usually in unstructured formats.[41] Big data is known as a large quantity of data that depends on the use of new and modern technological models and frameworks for the possibly of extracting its value through a process of its capturing and analyzing. And due to its voluminous size would never be possible to process effectively if using the traditional techniques. [42]

From a starting point, I will use this definition:

'Big Data is a term that refers to the enormous increase in access to and automated use of information: It refers to the gigantic amounts of digital data controlled by companies, authorities and other large organizations which are subjected to extensive analysis based on the use of algorithms. Big Data may be used to identify general trends and correlations, but it can also be used such that it affects individuals directly. [43]

According to Regulation no. 2016/679 of the Article 4, Para 1, of the General Data Protection Regulation (GDPR) on personal data.

'Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'.

[40] Tucker 'Has Big Data made anonymity impossible?' In: Big Data gets personal (MIT Technology Review, 2013). And Cumbley and Church 'Is 'Big Data' creepy?' (Computer Law & Security Review 2013) p 601–609.
[41] Douglas, Laney '3d data management: Controlling data volume, velocity and variety' (Gartner, 2001) p 02-06.
[42] Katal, Avita, Mohammad Wazid, and Rayan H. Goudar 'Big data: issues, challenges, tools and good practices' *Sixth international conference on contemporary computing (IC3)* (IEEE, 2013).
[43] European Economic and Social Committee (n 36) 36.

Big data is significant for analyst, policy makers and businesses to make better and critical decisions that were not possible in the past through its multidisciplinary framework.[44] Using figure 1 in explaining the big data structure would clarify different dimensions of the phenomenon.

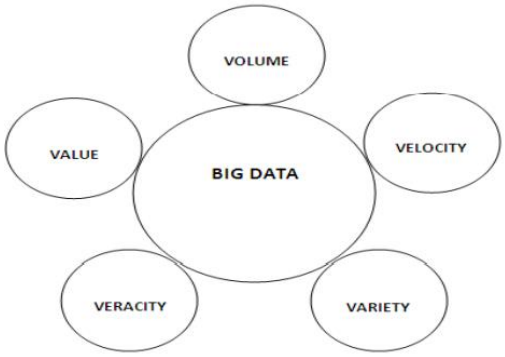


Figure 1: Structure of Big Data[45]

Following the definition provided by the IBM scientist which became more accepted, characterized big data by some features such as the 3V's (Volume, Variety and Velocity).[46] [47] But commonly depicted by five dimensions of big data, also known as the 5 V's structure, are as follows:

Volume - the size of data being accumulated from different areas at a rapid rate which shows the process of handling large scale of data with high dimensional databases.[48] An example of this is the social media platform such as the Facebook, and Instagram, where large numbers of photos are uploaded daily. There is a projection that this upload could reach a mind blowing size of 175 zettabytes every year by the year 2025.[49] The massive volume of data that are being generated and collected is voluminous, with estimates suggesting that the global data sphere will reach 35 trillion gigabytes by 2020.[50] Velocity – this is the speed at which data is being generated, accumulated and

[44] Vijayarani, S., and S. Sharmila 'Research in big data: an overview' (*Inf Eng Int J* 4, 2016) p 1-20.
[45]Ibid 2.
[46] Manyika et al. (n 34).
[47] European Economic and Social Committee (n 36) 36.
[48] Bormida, Marina Da (n 2) 73.
[49] The volume of data produced is growing quickly, from 33 zettabytes in 2018 to an expected 175 zettabytes in 2025 in the world (IDC, 2018).
[50] Qiu, J., Wu, Q., Ding, G. *et al.* 'A survey of machine learning for big data processing. (*EURASIP J. Adv. Signal Process'* 2016), 67 Available from https://doi.org/10.1186/s13634-016-0355.

processed because of the need for data to flow quickly for business needs for competitive advantage. Variety – big data comes in different formats; structured and unstructured forms and handling this type of forms requires a flexible storage system and supports processing solutions. [51]

Veracity – is the reliability and accuracy of data which is crucial because of the multiplicity of data and reliability on its authenticity. This makes it important to be able to verify, correct or delete unnecessary on incorrect data.[52] Value – the involves the extraction of valuable insights from the available big data, which is the main objective data analytics. This is the reason organizations put a lot of investments in the big data because they could derive value from them, through analytical system, trends and correlations for competitive advantage.

2.4. The 'Datafication' of the Society and Paradigm shift

The concept of 'big data' emerged from the need for data as more and more people in the society become engulfed in data, to live in a digital world. This need drove companies and organizations to find innovative ways of managing and handling the data growth that matches with it getting bigger, faster and voluminous, in different flexible forms.[53] The first time 'Big Data' became a term was in 1998 in a Silicon Graphics (SGI) by John Mashey, as it was seen in its growth to increase the storage capacity and processing power for large amounts of data used in examining and identifying certain hidden patterns and correlations for analytical purposes and insights.[54] [55]

Big data has been frequently used with no agreed definition as it has been used and associated with complex databases which are used in the operation of deducting important and useful insights that is crucial in making better decisions. So far, it can be said that big data goes more than the quantity of data in place but extends to the new and innovative dimensions of interpreting the available data and generating new ideas and knowledge useful for specific purposes.[56]

---

[51] Qiu, J., Wu, Q., Ding, G. *et al.* (n 50).
[52] Bormida, Marina Da (n 2) 71-91.
[53] Ishikiriyama, Célia Satiko and Carlos Francisco Simões Gomes (n 33).
[54] Vijayarani, S., and S. Sharmila (n 44) 1-20.
[55] Neelam Singh, Neha Garg, Varsha Mittal 'Data insights, motivation and challenges' (Volume 4, Issue 12, 2013) 2172, ISSN 2229-5518.
[56] Bormida, Marina Da (n 2) 77.

Living in the era of big data is characterized by governments, organizations and businesses developing the capacity to deduce many data that concerns people and their daily lives. The key aspect of this is the capacity of new technologies to capture, collect, store and process data in a faster, cheaper and more efficient ways with computational powers. This special ability with digital technologies has created the societal phenomenon known as 'datafication' that affects every aspect of everyone's life.[57] Undoubtedly, the importance of data is enormous and no area of our day to day activities are possible without the need and insights from data. This ever increasing importance of data for the economy and society is not yet done but has more to come as the future unfolds.[58]

This development has led to a new way of making vital decision or conclusions, known as 'Big Data paradigm' which depends on the aid of applied mathematical and statistical system on algorithms in analyzing and providing optimal solutions that are more advanced and better than humans.[59] Big data is crucial in helping us to understand the complexity of the society using the large amount of generated data as the society becomes more diverse, complex and advanced in technology.[60] Information such as the people's mobility, shopping and personal decisions made are accumulated, stored and with the advanced algorithms can make correlations of these stored data which can make predictable outcomes vital for making key decisions in business, governmental or any profitable venture through algorithmic patterns.[61] Data and applied statistics aid in predicting future events for both opportunities and risks which could give a sense and level of certainty for policy makers to rely on in making vital decisions.[62] It is thought that the mix of big data, computers and algorithms are capable in providing deep insights more reliable than experts in the field when it comes to models, theories and hypotheses.[63]

---

[57] Ibid.
[58] Ibid.
[59] Roger Koppl et al. 'Economics for a Creative World' 11 (J. INSTITUTIONAL ECON. 1, 4 2013).
[60] Geoffrey West 'Big Data Needs a Big Theory to Go with it' SCI. AM (2013) Available at https://www.scientificamerican.com/ article/big-data-needs-big-theory/ Accessed 12 May 2024.
[61] Mayer-Schönberger, Viktor, and Kenneth Cukier '*Big data: A revolution that will transform how we live, work, and think*' (Houghton Mifflin Harcourt, 2013).
[62] Ibid.
[63] Mark Graham, Big Data and the End of Theory? (THE GUARDIAN, 2012), available at https://www.theguardian.com/news/datablog/2012/mar/09/big-data-theory accessed 12 May 2024.

2.5. The Application and Implications of Big Data

The application of big data spans a wide range of sectors and disciplines for business, healthcare and scientific research fields and even urban planning and development. For example,

In business sectors, the volume of business data doubles in every 1.2 years.[64] Many businesses are using big data in making vital decisions for the growth and expansion. In searching for more competition and sales, companies such as Wal-Mart partnered with technology firms such as HP (Hewlett Packard) for more on warehousing which could reduce cost for Wal-Mart offer convenience and customer satisfaction.[65] Using big data analytics can assist businesses in identifying new business and market opportunities which could give them a competitive edge over others not utilizing the opportunities available in the big data trend in enhancing customer experience, fostering strategic business decisions and maximizing operational efficiency.

Using big data in the healthcare industry can enhance disease prediction pattern to limit the impact of outbreak and public health emergencies, optimizing personal health treatment and plans while improving patient treatment and outcomes. [66] In the area of urban planning and development, big data can help in addressing societal challenges associated with transportation, reducing the climate change effects and improving the outcomes of education and personal development.[67] Big data plays crucial role in public administration, large populations comes with diverse and complicated needs and the governments must deliver effectively and efficiently. Large number of data is created through different services that ranges from public health services, children and youth learning, health care services for the senior citizens.[68] In harnessing the potential benefits of this reality and solving keys issues facing the government using big data, governments such as the United States Library of Congress through the gathered 3 TB of information, inspired the launch of a $200 million plan for Big Data research and Development by the Barack Obama Administration.[69] As a

[64] Manyika et al. (n 34).
[65] Hashem, Ibrahim Abaker Targio, et al. (n 65) 98-115.
[66] Miron-Shatz, T., A. Y. S. Lau, C. Paton, and M. M. Hansen (n 65) 21-26.
[67] Ibid.
[68] Hashem, Ibrahim Abaker Targio, et al. (n 65) 98-115.
[69] Kim, Gang-Hoon, Silvana Trimi, and Ji-Hyong Chung 'Big-data applications in the government sector' *Communications of the ACM* 57.3 (2014) p 78-85.

major concern for many governments, the Japanese government in its Big Data development program, saw that this could be a useful weapon for its national scientific programs.[70]

In its report on big data, 'Big Data for Development: Challenges and Opportunities' the United Nations highlighted the key concerns about big data and how to promote the global conversion related to the use of Big Data for global progress. The European public sector has seen a significant decrease in the cost of its administrative expenses from 15 – 20 percent and saving a whooping amount of money through big data applications.[71]

Scientific research sectors have become more advanced and data driven, key areas such as bio-informatics, social computing and meteorology are heavily relying on big data for making critical decisions through analytical insights gathered from big data.[72] [73] The need_and demand are insatiable and poses a critical question of what the implications could be when things are not done properly and ethically by big data controllers such as the big data companies and governments. In political sciences and monitoring, there is an increasing demand for critical insights on the nature and public voting patterns which is key to the success or failure of elected officials. Different data methods are being used to collect data from potential voters to determine their personal choices.[74] This habit is common to the United States where polling is used as a morale boost or indicator of likeability of political candidates.

Internet of Things (IOT) is the global center and marketplace of the big data applications. Ranging from business venture to GPS services, the IOT, new and advanced technologies are making data driven applications and decisions to support our everyday activities and needs.[75] While the IOT is with opportunities and challenges, it is important for the structure of key future financial information, and communication technology for global network.[76]

---

[70] Oussous, Ahmed, et al. (n 70) 431-448.
[71] Hashem, Ibrahim Abaker Targio, et al. (n 65) 98-115.
[72] Szalay, Alex 'Extreme data-intensive scientific computing' *Computing in Science & Engineering* 13.6 (2011): 34-41.
[73] Bryant, Randal E 'Data-intensive scalable computing for scientific applications' *Computing in Science & Engineering* 13.6 (2011) p 25-33.
[74] Oussous, Ahmed, et al. (n 70).
[75] Perera, Charith, et al. 'A survey on internet of things from industrial market perspective' (*IEEE Access* 2 ,2014): 1660-1679.
[76] Acharjya, Debi Prasanna, and Kauser Ahmed. 'A survey on big data analytics: challenges, open research issues and tools' *International Journal of Advanced Computer Science and Applications* 7.2 (2016) p 511-518.

2.6. Legal and Ethical Considerations in Big Data

There is a growing concern on the legal and ethical implications about the use of big data as its prevalence is continuously growing. The massive collection, storage, and analysis of personal data imply important privacy issues, because of the low level of awareness on the part of individuals of how their data is being used and the possible consequences that these activities could be. Additionally, issues of data ownership, consent, and the potential for algorithmic bias and discrimination have become increasingly important considerations.[77] Researchers and policymakers have emphasized the need for robust data governance frameworks, comprehensive privacy protection laws, and ethical guidelines to ensure the responsible and equitable use of Big Data. [78]

It is important to know the place of big data and law in the society, to find reliable and effective ways to protect privacy rights and data protection. In lieu of the fact that big data is opposed to the rule of law in some ways because of the 'syntactic' nature of big data and 'semantic' nature of the rule of law.[79] While law is a value- based and abstract, big data is different because of its empirical, algorithmic and deterministic characteristics, it relies on human for standards and boundaries,[80] as only human can change their perspectives as the environment changes. This makes legal principles an important component for data privacy and protection. Even the most advanced machine learning technology does not have the capacity to inform us of relevant factor and new challenges beyond the information imposed on it by its creators.[81] In consideration of big data and law, the fundamental difference between the law systems is one of the important aspects in data protection and privacy. Big data' evolution is creatively unpredictable and could go beyond its original purpose of creation.[82]

This failure of the objective test is a key factor why big data will not meet the basic purpose of the legal system. With this difference, big data would bypass the concept of consent if such actions

[77] McNeely, Connie L., and Jong-on Hahm 'The big (data) bang: Policy, prospects, and challenges' (*Review of Policy Research* 31, no. 4 2014) p 304-310.
[78] Miron-Shatz, T., A. Y. S. Lau, C. Paton, and M. M. Hansen (n 66) 21-26.
[79] Devins, Caryn, Teppo Felin, Stuart Kauffman, and Roger Koppl. 'The law and big data' (*Cornell JL & Public Policy* 27, 2017) p 360.
[80] Hale, Sandra 'The discourse of court interpreting' [2004]: 1-288.
[81] Devins, Caryn, Teppo Felin, Stuart Kauffman, and Roger Koppl (n 79).
[82] Ibid.

were not regulated by law through set obligations and standards for big data creators to uphold. As big data imposes algorithmic kind of method that produces an organized but highly problematic outputs and challenging lack of accountability and transparency to the law. So, reliance on big data for decision making by policy makers could be problematic as it is based on mere correlations picked up by data with limited and unclear causal relationships. The lack of proper definition and identification of facts and the designs used in data interpretation could be biased in uncertain ways and will end up influencing the outcomes or end products.[83] the lack of evidence based facts, big data designed approaches might bypass the authority of the administrative and legal systems to manipulate the society.[84]

Ethically, big data analysis involves interconnected aspects which are the theoretical – which is the philosophical aspects including the rights and acceptable of big data, and the pragmatic aspects - the impacts of big data on users.[85]

According to Professor Floridi, in 'The Fourth Revolution' views the big data issues as one that shows a new frontier of innovation and competition which has the capacity of creating new businesses and companies and new research insights or problems for any country by extending the limits of events in predictable and expectable ways.[86] However, the key aspect of ethics on big data lies in data protection – privacy, freedom and discretional rights of the individual. These are important to the need of an individual but in contention with the societal needs when it comes to the privacy of the individual and security of the society or state.[87]

The state's right to access private data of the individual because of public security concerns such as terrorism, public health emergencies and serious crimes. These actions are authorized by law when necessary for the specific purpose of the state under the Article 8 of the European Convention on Human Rights. Ethical challenges are always a concern when it comes to the use of big data by data controllers. More ethical issues that could arise when big data is exploited are as follows:[88] The artificial intelligence algorithm bias, Privacy rights, Data purpose limitation, User digital

[83] Ibid.
[84] Ibid.
[85] European Economic and Social Committee (n 36) 36.
[86] Floridi, Luciano 'The fourth revolution: How the infosphere is reshaping human reality' (OUP Oxford, 2014).
[87] European Economic and Social Committee (n 36) 36.
[88] European Economic and Social Committee (n 36) 36.

profile, Personal capabilities and freedom, Shared rights between data subjects and exploiters, Tailored reality and filters

2.7. Data Privacy and Data Protection

There is an increasing use and dependance on big data for daily activities. However, this has not reduced the challenges that arises from the data users. If the use of big data is not properly and safely processed by data controllers, there will be potential threat and possible breach of the privacy rights of data subjects. The datafication of the society is has seen every aspect of ours lives integrated into the digital platforms, which is made possible by the intelligence and capacity of new technologies to capture, collect, store and process data in a faster, cheaper and more efficiently, in flexible patterns with computational powers.[89] As more people are living in the digital spere, such as using the smart phones for everyday needs, challenges of privacy arises due to the accumulation of personal data, and challenges of security for data users. The ease of using smart technologies at one's convenience in managing daily activities could bring a serious security issues to the data user, if the access and control is lost unintentionally and illegally to the wrong people.[90]

With datafication, the ever increasing reliance on the digital platforms exposes data subjects to potential breach of data privacy and rights.[91] Also, the use of algorithms and artificial intelligence operational designs break the traditional data encryption order is a rising challenge to data security.[92] The rise of data clouds makes data storage easier, at the same time poses a security risk of being exposed to cyber attacks and hackers and individual data privacy violated and exposed to other potential security risks. Common examples are the Wikileaks, Panama papers, Ransomware and Cambridge Analytica where data subjects limited rights to their stored data, which had been secured consensually with assurances of security, secrecy accessibility and integrity being violated by cyber attacks.[93]

---

[89] Bormida, Marina Da (n 2).
[90] Zhang Dongpo 'Big data security and privacy protection' *8th international conference on management and computer science* (ICMCS, Atlantis Press, 2018).
[91] Chenthara, Shekha, Hua Wang, and Khandakar Ahmed 'Security and privacy in big data environment' (2018).
[92] Smid, Miles E., and Dennis K. Branstad 'Data encryption standard: past and future' (Proceedings of the IEEE, 1988) p 550-559.
[93] Chenthara, Shekha, Hua Wang, and Khandakar Ahmed (n 91).

2.8. Big data and its Impact on Human Rights

As big data increasingly becomes a key area that enables economic growth and development, it comes with serious concerns with regards to privacy rights and data protection. Emerging new threats from data gathering methods, big data usage and governments security surveillance.[94] Even though the European legal framework on data – the GDPR, has been one of the most effective data privacy and protection mechanism. It is no doubt that societies of today are in for a transformational time as more areas of daily activities and decisions are made based on the algorithmic conclusions.

The 'creep factor' of big data whereby data controllers manipulate data for unclear and undefined reasons poses a great risk to data privacy and security. Especially, now that the digital information is the new oil for economic growth and societal transformation.[95] This new gold standard for wealth creation is digital, global and borderless with negligible international consensus on the modus operandi, ethics and acceptable norms.[96]

As big data becomes an undeniable part of the human daily life and the most valuable commodity replacing the oil, it becomes an imperative to find effective legal mechanism for responsibility and accountability. So far, it has been difficult for the nation states to handle the impacts of the 'politics of big data' – the data that is collected, who owns it, what it is for and how it should be used, within their jurisdiction authorities, which could be a result of the outpaced rate of technological growth unmatched with the post - industrial regulatory frameworks.[97] With the European legal framework for data privacy and protection and the increasing datafication of the society, it becomes crucial for a continuous effort in matching the pace of technological growth with the regulatory framework that is compliant for the current information age.

Following the big data paradigm, that is using the existing traditional framework with systemic loopholes such as using data subjects informed consents beyond the data processing purposes.[98] The fragmented and fractured national rules for data privacy and protection, requires to be assessed for upgrade for a more effective legal framework worthy of the emerging responsibilities and

[94] Bormida, Marina Da (n 2).
[95] Nersessian, David (n 1) 845-854.
[96] Ibid.
[97] Ibid.
[98] Bormida, Marina Da (n 2).

accountability. In view of the ethical and social dimensions of big data challenges, there is a need to evaluate this area in the context of ethical frameworks for protecting human rights and dignity and to ensure that the data paradigm is in congruent with ethical values of the society. Balancing the need of big data for both businesses and citizenry comes with much effort. This is acknowledged by the European Data Protection Supervisor (EDPS) as a huge responsibility that requires the right data protection mechanisms in place.[99] The EDPS stated the need for the respect for human dignity and its correlation with the respect for 'the right to privacy and the right to the protection of personal data', which under the European Charter of Fundamental Rights, are 'inviolable rights'.[100]

The implications of big data technologies on human dignity goes beyond the group privacy and profiling but using advanced systems of discrimination based of accumulated data and automated decision making.[101] Irrespective of the economic benefits of the use of big data by organizations seeking economic insights and better decision making, the big data paradigm comes with personal risks due to unethical and intentional actions to escape the original intentions of the privacy law such as enshrined in the data protection laws of the GDPR.

In Marina da Bomida's article, on the '*Big Data World'* additional risks of the 'creepy factor' of the big data extends to the following privacy and security challenges.

Data breaches and privacy obstruction – this unethical practice can compromise privacy, by passing the intent of privacy laws. Using the advances in data analysis has shown that previously private data could lead to targeted customer profiling. Re-identification risks can occur, even after the anonymization of the data subjects. Using advanced de-anonymization technologies can re-identify and re-trace the original data subjects. Powerful insights from multiple datasets have the capacity to identify personal data and its owners, this action poses a grave risk to privacy concerns, without the consent of the data subjects. Big data use lack the adequate transparency as data subjects find it difficult to control access to their private data, a clear breach of their civil rights.

In view of these, it is the intent of the GDPR to maintain the right to privacy and data protection. It is the onus of the big data companies and other data controllers to ensure trust, privacy and data

[99] Ibid.
[100] Ibid.
[101] Ibid 76.

protection. By assessing the legal responsibilities and accountability mechanisms, it aligns with the obligatory part of the law to upgrade the existing legal mechanisms to match with the advances in the big data era.

2.8. Conclusion

Theoretically, the ethical use of big data is of immense importance for appropriate use of big data in an increasing era of digital dependance. In using socio-legal methodology, an interdisciplinary approach that looks at the intersection of law and the broader social contexts. This chapter has identified the keys concepts of big data, and its interrelated concepts with data controllers such as big data companies and other entities. It stressed the ethical and legal importance of data privacy and data protection and its implications. Also, defining its meaning, phenomena and the relationships between them with the existing legal framework and the legal loopholes that allows potential breach of one of the basic principles of human rights. By following these steps and making the relation clearer.

The next chapters will explore the legal obligations and accountability mechanism of big data companies with special focus on the European Convention on Human Rights. Examining its Challenges and opportunities, and making recommendations for policy makers, researchers for further research on this topic.

CHAPTER THREE - The European Convention on Human Rights (ECHR)

3.1. Introduction

The ECHR became a milestone achievement in human rights protection for the European states, which provides important safeguards for individual freedoms, and set up the legal mechanisms that allows enforcement and accountability.[102] While the ECHR is considered as a significant mechanism for individual rights safeguards, it was not set up during the time of technological advancement. Recent developments in emerging technologies that have become prevalent in individuals' daily lives and relationships with the outside world must not have been envisioned during the development of the ECHR. Although, additional legal mechanisms for data control emerged, such as the GDPR. However, the rate of technological development need to be matched with effective legal mechanism if the individual rights and accountability will prevail. One of the keys areas of focus is the data controllers, as digital technologies increasingly advance. So, the significance of the ECHR extends to the responsibilities of big data companies in maintaining ethical data process and upholding these fundamental human rights. [103]

The ECHR as an international treaty was drafted and established by the Council of Europe in 1950, to protects human rights and fundamental freedoms in Europe. The ECHR came into force in 1963 while the ECtHR was established in Strasbourg to hear cases of violations of rights according to the provisions of the ECHR. The place and role of the ECHR and ECtHR are important in fostering democratic health, the rule of law and respect for human rights in the member states.

While the ECHR sets a list of comprehensive sets of human rights and freedoms for each of the member states must uphold, it also established an arbiter for the interpretation and enforcement of the Convention's provisions. Since its inception, the Court has been able to develop a body of case laws, such as the 'margin of appreciation', this allows it in dealing with complex legal and

[102] Gasser, Urs, and Virgilio AF Almeida 'A layered model for AI governance' (IEEE Internet Computing 21 no 6, 2017) p 58-62.

[103] O'Donnell, Thomas A 'The margin of appreciation doctrine: standards in the jurisprudence of the European Court of Human Rights' (Hum. Rts. Q. 4 1982) p474.

jurisdictional state issues, allowing states the flexibility in applying Convention's provisions based of the unique state needs.

To answer the key question of this study on the legal responsibilities that big data companies have on individual privacy rights, this chapter will explore the key provisions of the ECHR for enforcing obligations and accountability available for big data companies. It will evaluate the correlation between the privacy rights, the scope of the freedom of expressions and the right to effective remedy when any of the fundamental rights are breached. Also, there are separate accountability mechanisms companies can initiate independently in lieu of their obligations to ensure data protection and respect for the rights to privacy. The role and authority of regulatory bodies are vital to data protection and one of the centers of the European regulatory centers for the protection of the right to privacy within Europe.

3.1.1. Background of the ECHR

The European Convention on Human Rights is one of the premier human rights instruments modelled after the Universal Declaration of Human Rights (UDHR) shortly after the end of the World War two (WWII).[104] As a result of the heavy loss of lives and gross violation of human rights during the war, it becomes an imperative for the international protection of human rights, which the European Convention for the Protection of Rights and Fundamental Freedoms became one of the major legal framework for the protection of human rights. Earlier focus were centered around four freedoms; the freedom of life, the freedom of religion, the freedom of want and freedom from fear.[105] In spite of many challenges of its efficacy due to allure of national socialism of that period.

The General Assembly of the United Nations in May 1948 adopted the UDHR, an important milestone that further motivated the 'Congress of Europe' in the Hague to set up a legal framework for democratic states as a standard of conformity on the protection of human rights in their

[104] Van Dijk, Pieter, and Godefridus JH Van Hoof. *Theory and practice of the European Convention on Human Rights* (Martinus Nijhoff Publishers, 2023) p 1.
[105] Ibid.

respective authorities. What followed were the inception of what would be known as the European Convention of Human Rights and its judicial arm, the European Court of Justice.[106]

3.2. The Key Provisions and Mechanisms for Enforcement and Accountability Under the ECHR

This part is important in elaborating the study question of how the ECHR will be useful in the enforcement of these individual privacy rights. And how the principles such as Article 6, Article 8 and Article 10 apply to big data companies processing personal data.

Under the Article 1 of the ECHR, member states are obligated to guarantee the rights and freedom of everyone in their jurisdiction. Article 1 does not imply any limitations on the authority or sovereignty of the member states. But sets a boundary between the concept of authority of the state and the responsibility it guarantees even beyond its borders. An important factor of the technological advancements that poses a threat to individual rights is the big data and advanced analytics. This must be continually evaluated in lieu of the established rights and freedoms under the ECHR. [107]

Biological identity issues, biomedical studies and other key data driven sectors have been identified in the GDPR, which has been a global example in individual privacy and data protection. Extensively, the ECHR key Articles for the right of privacy (Article 8), the right to the freedom of expression (Article 10) and the right to an effective remedy (Article 13) embodies the main bearings for the accountability of the big data companies and data controllers.

The ECHR is comprised of several key provisions which established the fundamental human rights and mechanisms to enforce and ensure the accountability of these rights and freedoms.

[106] Ibid.
[107] Politou, Eugenia, Efthimios Alepis, and Constantinos Patsakis. 'Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions' (Journal of cybersecurity 4, no 1, 2018) 01.

Article 2: The right to life protects individuals from unlawful deprivation of life. This provision imposes an obligation on member states to safeguard the lives of individuals within their state's authority.

Article 3: The prohibition of torture prohibits the use of torture, and other inhuman or degrading treatment. This right is considered and absolute right with no derogations or exceptions.

Article 6: The right to a fair trial ensures the right to a fair and public hearing by an independent and impartial tribunal set up according to the law within a reasonable period.

Article 8: The right to private and family life protects the individual privacy and their family life, home and correspondence from arbitrary interference by the government or any other public authorities.

Article 10: The freedom of expression guarantees the right to the freedom of expression, which includes holding personal opinions and to receive or impact information and ideas without the interference of the public authority.

Article 13: The right to an effective remedy ensures that the right to an effective remedy before national authorities for any breach of these rights under the ECHR.

Individuals can bring cases before the ECtHR if other alternative ways of remedies fails in the member states. The ECtHR judgement is binding on the member states. These judgements must be executed by the member states to rectify any breach of the Convention. For this research, I will elaborate more on three key articles (Article 8, Article 10 and Article 13).

3.3. Legal Responsibilities of Big Data Companies Under the ECHR

There are many national and regional laws that regulates big data companies within the context of Pan European and European Union legislation. This research will look at the most comprehensive of the them such as the GDPR and the ECHR provisions. Big data companies have the responsibility of ensuring that the data collected, processed, and disseminated will not breach the human rights which are protected under the provisions of the ECHR. These responsibilities includes the privacy of individuals (Article 8), ensuring the right to the freedom of expression

(Article 10), and making sure that there is effective remedies if any of these rights are violated (Article 13).

3.3.1. International Framework

Before looking at the responsibilities under the ECHR, I will give an overview of the key international legal framework and the regional regulations, GDPR. This is vital in making a comprehensive analysis and the relevance of the ECHR in big data protection, especially in legal binding agreements and explicitly.[108]

Under the international legal framework, there is no legally binding multilateral agreement on big data, but just multilateral commitments by member states that stipulates the responsibility to respect human rights and the right of privacy.[109] It is important to note that the ECHR drew its motivation and was established after the UDHR following the end of World War II in 1948. However, the United Nations did not explicitly mention data protection in the UDHR but it can be said that the protection of data within the context of human rights as privacy right is enshrined in Article 12 of the UDHR:

'No one shall be subjected to arbitrary interference with the privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks' United Nations.' (UN) (1948)

The right of privacy against interference from unjustified authorly marks the beginning of individual right recognition by member states at the international level, although it is non-binding, it had impacted international relations and further development of regional conventions, declarations and resolutions and laws on human rights such as the ECHR in Europe.[110]

3.3.2. Regional Framework

Following the United Nations UDHR is the European Convention on Human Rights with similar and different provisions of rights and freedoms. With the right to personal data protection in Article

[108] Lenz, Rainer 'Big Data: Ethics and Law' SSRN Electronic Journal 10.2139/ssrn.3459004 (2019) p 15.
[109] Ibid.
[110] Ibid 16.

8 of the Convention under the 'right to respect for private and family life' of the ECHR. The rights and freedoms under the ECHR are binding multilateral legal framework unlike the UDHR and has the ECtHR to ensure compliance and accountability of any breach of the convention's violations.[111] Governments and citizens can turn to the services of the ECtHR if the national legal framework for accountability fails.[112] List of cases examined by the court includes data protection issues such as surveillance carried out by the government authorities and private companies, interception of communications and personal data storage without the consent of data subjects.[113]

The Council of Europe (CoE) (2018 p 23), handbook of European Data Protection Law states that the right to privacy is not an absolute right:

> *'The respect for private life is not an absolute right, as the exercise of the right to privacy could compromise other rights, such as freedom of expression and access to information and vice versa. Hence, the Court strives to find a balance between the different rights at stake'.*

It highlights the balance between privacy and other rights such as freedom of expression and access to information, this is important in ensuring that the exercise of one right would not impede the others.[114] There are five EU regulations and directives on data protection, but the key point to note is that they have different objectives.[115] It is crucial for this research to identify the key legal mechanisms that is instrumental for individual privacy rights and data protection. Outside the ECHR provisions, the GDPR is vital for the protection of individual data privacy and security.

The EU General Data Protection Regulation has seven key principles:

1. Lawfulness
2. Transparency
3. Fairness

[111] Ibid 17.
[112] Ibid.
[113] Ibid 19.
[114] Giakoumopoulos, C., G. Buttarelli, and M. O'Flaherty 'Handbook on European data protection law *Luxembourg:* (Publications Office of the European Union 2018*) https://doi. org/10.2811* 58814.
[115] Lenz, Rainer (n 108) 19.

4. Purpose limitation
5. Data minimization
6. Accuracy
7. Storage limitation
8. Integrity
9. Confidentiality.

These principles offers data subjects the right for data sovereignty and ownership over the use of their data.[116] Apparently, there are instances where big data applications do not work in congruent with the principles of the GDPR.[117] I think that this situation creates a loophole for potential breach of the right to privacy and data protection. And was highlighted by the General Advocate (GA) and jurisprudence of the European Court of justice (ECJ) citing the limitation of the GDPR scope and personal data definition.[118] The Article 4 of the GDPR states.

> *'Article 4 GDPR Definition: (1) personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'.*

According to the European Court of Justice, the personal data is the only data that is identifiable to the data subject, such as the *'name, date of birth, nationality, gender, ethnicity, religion and language'.*[119] The GDPR regulation does not cover activities such as restructuring, analyzing, and combining different sets of sensitive data for business purposes, and big data processes within this context are not seen as a violation of the rights of data subjects, because it is GDPR compliant.[120] In this process, data subjects are exposed to possible severe threats to their data rights and freedom.

[116] Ibid 20.
[117] Ibid.
[118] Ibid.
[119] Wachter, S., & Mittelstadt, B 'A right to reasonable inferences: re-thinking data protection law in the age of big data and AI' (Columbia Business Law Review,2019).
[120] Ibid 20.

The definition of personal data under the GDPR as being static does not match with the reality of the emerging nature of personal data. According to the GDPR definition, the correlation of data sets, the possibility that a person can be identifiable and trackable, allows the process of de-anonymization of data.[121] However, the nature of data is gradually changing from its static form and poses challenges to the 'GDPR compliant' form of data definition as a static idea. Different types of data such as personal data, sensitive data, private data and statistical data go through a process from anonymization, de-anonymization and pseudonymization.[122]

It makes the GDPR definition of data limited in scope and creates loopholes for potential risks to personal data privacy. This could be utilized by big data companies for their business advantages without following proper ethical rules. The focus of the GDPR is for personal data protection, and under the Article 8 of Charter of Fundamental Rights of the European Union, which is complementary to the Article 7 of the Charter on ePrivacy Regulations, the focus is on person's private and family life, it has a broader scope that protects both the natural person and legal person unlike the GDPR. So, the ePrivacy allows metadata's broader use of combined data for analysis and interferences. Which big data companies use for obtaining insights vital for critical decision making for business advantage and policy making.[123] These highlights crucial areas of concern in data privacy and protection.

According to Wachter and Mittelstadt (2019), the is a need to rephrase the concept of privacy in data protection to be in congruent with the provisions of the ECHR, the Council of Europe's 'Modernized Convention for the Protection of Individuals with Regard to the processing of personal data and their guidelines on AI'.[124] This update version focuses on the emerging technologies such as the artificial intelligence (AI) and to ensure that there is adequate measure in place to curb unwanted consequences that could breach the fundamental principles of human rights – the right to privacy and data protection.[125] The guidelines on AI sets the legal framework for applying the Conventions principles within the context of AI and big data. The relevance of

[121] Lenz, Rainer (n 108) 20.
[122] Van der Sloot, B., & van Schendel, S 'Ten questions for future regulation of big data: A comparative and empirical legal study' J. Intel Prop Info Tech & Elec Com (2016) p 7, 110.
[123] Lenz, Rainer (n 108) 20.
[124] Wachter, S., & Mittelstadt (n 119) 81.
[125] Council of Europe (CoE) 'Handbook on European data protection law' (2018) Available at https://www.echr.coe.int/Documents/Handbook_data_protection_02ENG.pdf Accessed 10 July 2024.

this development is that it shows the concern of technological implications and the importance of responsibility and accountability mechanisms. Also, the importance of fairness and transparency in emerging AI systems to ensure that individual rights and freedoms are protected.[126]

Following the definition and distinction of sensitive and non sensitive personal data in the Article 4 of the GDPR, big data applications are irrelevant because of the objective of the data protection being on the input.[127] While the input of the data is important, it is crucial for law makers to pay attention on the output when the processed combined data comes out differently and used for other purposes such as making decisions and inferences.[128] Therefore, it is important to apply a balanced approach that carefully considers the human rights perspective of data processing, or 'data processing with a human face'.

3.4. Privacy Rights (Article 8), Interpretation and Scope, Freedom of Expression (Article 10), Right to an Effective Remedy (Article 13)

3.4.1. The Right to Privacy

The scope of Article 8 of the ECHR includes that of personal data and private life. According to the ECtHR, it is necessary to protect the individual from any form of intrusion to their privacy from state and non - state agents such as the big data companies. It is the onus of companies to adhere to their obligatory duties and ethics to ensure an effective privacy and data protection.[129]

Under Article 8 of the Convention - The Right to respect for private and family life:

1. '*Everyone has the right to respect his private and family life, his home and his correspondence.*

2. *There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for*

[126] Ibid.
[127] Lenz, Rainer (n 108) 23.
[128] Ibid.
[129] Guide on Article 8 of the European Convention on Human Rights "Right to Respect for Private and Family Life" European Court of Human Rights (2024) p 7.

the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.'

The key points under Article 8 are: Private life: this included personal autonomy, physical and psychological integrity, and the right to allow one to establish relationships with others. This concept covers the right to establish personal identity and form relationships.[130] It allows one to participate in vital economic, social and cultural activities.[131] This right protects one from media and outside interference on personal communications such as personal records, photos, letters, diaries. Any access to these must be done with the consent of the owner.[132] Family life: The right to family life under the Article 8 of the ECHR includes relationships that are between families and including ones that are not based on marriage such as unmarried couples, adopted and adoptive parent, foster and fostered child. Home: including the right to enjoy your family without unwarranted interference. Public authorities should not enter your home without permission. Correspondence: the right to the protection of all kinds of family communications.

Restrictions of the right under Article 8 of the ECHR There are some situations that could allow the public authorities to interfere with the right to private and family life, home and correspondence. Interference is allowed within the context of certain actions that are considered lawful, necessary and proportional under the law to protect the following: National security, public safety purposes, The economy, Health or morals, The rights, and freedoms of others, and prevent crime or disorder in the society.

3.4.2. Article 10 of the ECHR: The Right to Freedom of Expression

The scope of Article 10 of the ECHR guarantees the rights and freedom of expression. This concept of right includes the right to hold personal opinions, receive and impact information and ideas. It is important to acknowledge the vital roles big data companies play in the facilitation of the flow

[130] Article 8 of the ECHR 'Respect for your private and family life' Equality and Human Rights Commission EHRC (2021) Available at equalityhumanrights.com [Accessed July 20, 2024].
[131] Ibid.
[132] Ibid.

of information. However, this is a need to balance this flow of information with the prevention of harmful and unlawful contents shared through their platforms.[133]

Under the Article 10 of the ECHR:

1. *'Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.'*

2. '*The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.'*

The right to hold personal opinions, receive and impact information and ideas might be gained through public protests and demonstrations. Additional avenues of expression could be done using different types of publications, public media channels, artistic expressions, the internet or radio broadcasting.[134]

Restrictions to Article 10 of the ECHR includes the responsibility to respect other people's right of expression or rights, even though you have the right to expression. It is important to know where the border to this freedom lies. This means that the balance between one's freedom of expression and others is in respecting others. An example of this kind of restriction is when a person's freedom of expression inspires racial or religious hatred. And actions taken by the public authority to restrict this kind of expression must show that it is 'proportionate'.[135] The interference of public authorities on this right of expression must be done whenever there is a proof that the action carried is lawful, necessary and proportionate to carry the following tasks:

[133] Article 10 of the ECHR 'Freedom of Expression' Equality and Human Rights Commission EHRC (2021) Available at equalityhumanrights.com [Accessed July 20, 2024].
[134] Ibid.
[135] Ibid.

To protect the national security, territorial integrity of the states or to maintain public order., to prevent crime or disorder, to protect health or morals, to protect the rights and reputations of other people, to maintain the authority and impartiality of judges, and to prevent the disclosure of confidential information.

3.4.3. Article 13 of the ECHR: The Right to an Effective Remedy

This provision ensures that there is an effective remedy when any right of the Convention is breached. This creates a framework for accountability and enforcement.

According to Article 13 of the Convention:

'Everyone whose rights and freedoms as set forth in [the] Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity'.

In lieu of this. Big data companies are obligated to ensure that individuals have access to address their grievances with regards to any of the provisions of the ECHR, such as breach of the right to privacy, complaints on lack of transparency and efficacy of the regulatory agencies.[136] The objective of Article 13 is to ensure that individual's whose Convention rights have been breached, could get relief from their national jurisdictions, before seeking a redress from the international court, which is the ECtHR. In other words, the primary responsibility to the protection of the Conventions rights is the onus of the member states.[137] The Kudla vs Poland [GC] 2000 & 152 is an example of this objective, decided by the ECtHR, founding the violation of Article 3, 5,6 of the ECHR. The significance of the case is the obligation to ensure that detainees receive adequate care, and the need for timely judicial proceedings and remedies when any of the Convention provisions is breached.

3.5. Accountability Mechanisms of Big Data Companies

There are many ways to hold big data companies accountable and that should be through the available combination of legal, regulatory and independent company's ethical mechanisms. This

[136] Council of Europe: European Court of Human Rights, *Guide on Article 13 of the European Convention on Human Rights - Right to an Effective Remedy* (2020) p 84.
[137] Kudla vs Poland [GC] 2000 & 152.

section will identify the accountability mechanisms that can be used to enforce compliance under the ECHR framework.

Legal Mechanisms: The legal mechanisms includes the national courts and ECtHR mechanism which allows judicial process where individuals whose rights and freedoms under the provisions of the ECHR have been violated, could possibly seek redress. Articles 13 of the ECHR ensures the efficacy of this legal mechanism.[138]

National Courts are the first point of call for the defense of rights and freedoms for the right of privacy. Redress is done within the national courts where both national and incorporated international human rights norms could be applied.[139]

European Court of Human Rights based at Strasbourg, France, comes into the rescue, when national legal remedies have been exhausted. The ECtHR ensures that the provisions under the ECHR are implemented for the member states. Individuals can approach this court with cases that could not be redressed at their national courts.[140]

Regulatory mechanisms: Regulatory Bodies are important in ensuring the right to privacy and data protection. European member states have data protection authorities (DPA's) whose primary responsibility is to enforce compliance of the data protection laws such as the General data Protection Regulation (GDPR) and other key provisions of privacy rights under the ECHR.[141] The DPA's ensure that big data companies and other data controllers comply with the legal requirements of the existing legal mechanism.[142] The Article 8 of the ECHR plays a crucial role in interpreting and enforcing data protection norms, because of its provisions for the right to respect private and family life.

---

[138] Marko Bošnjak, Kacper Zajac 'Judicial Activism and Judge-Made Law at the ECtHR' (Human Rights Law *Review* Volume 23 Issue 3, 2023) Available at https://doi.org/10.1093/hrlr/ngad015.
[139] Ibid.
[140] Laurence R. Helfer 'Redesigning the European Court of Human Rights: Embeddedness as a Deep Structural Principle of the European Human Rights Regime' *European Journal of International Law* Volume 19 Issue 1(2008) P 125–159, https://doi.org/10.1093/ejil/chn004 .
[141] Guide on Article 8 of the European on Human Rights ' Right to Respect for Private and Family Life' (European Court of Human Right, 2024) p 7 https://rm.coe.int/guide-on-article-8-of-the-european-convention-on-human-rights/16808e67cb
[142] Case-Law of the European Court of Human Rights Data Protection. https://rm.coe.int/guide-on-article-8-of-the-european-convention-on-human-rights/16808e67cb

3.6. Regulatory Frameworks and Bodies

Regulatory agencies are crucial for safeguarding the right to privacy and data protection. There are many regulatory frameworks that ensure that the activities of big data companies are in congruent with the provisions of the ECHR.

General Data Protection Regulation: This provides one of the most comprehensive legal frameworks for data protection within the European union in alignment with the principles of the ECHR.[143] The key points of the GDPR in regulatory framework are:

Comprehensive framework with penalties for non-compliance – Through the GDPR, it ensures that personal data is processed adequately with care and respect in line with the Chapter II, Article 5 on principles of data processing.[144] When a data controller such as big data companies fails to compliance, it faces the penalty of paying a huge fine of up to 20 million Euros or 4 percent of the annual global turnover of the company.[145]

In congruent with the ECHR – The GDPR aligns the principles of the ECHR with key provisions that focuses on data protection and the right to privacy such as Article 8 of the ECHR. The GDPR grants individuals with some rights such as the right to access to their personal data, the right to erasure and the right to data portability.[146]

Key principles of the GDPR includes lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, integrity, storage minimization and confidentiality.[147] **Accountability and compliance** of organizations with the GDPR principles are mandatory, because of data processing requirements. It is a requirement for organizations to appoint Data Protection Officers (DPO's) for Data Protection Impact Assessments (DPIA's) which helps in evaluation and auditory data processes.[148]

---

[143] Kuner, Christopher, Lee Bygrave, Christopher Docksey, and Laura Drechsler '*The EU general data protection regulation: a commentary'* (Oxford University Press, 2020) Available at: https://global. oup.com/academic/product/the-eu-general-data-protection-regulation-gdpr-9780198826491.
[144] Ibid Chapter II Article 5 of the GDPR p 67 – 69.
[145] Ibid Chapter IV Article 24 of the GDPR.
[146] Ibid 87 Chapter III Article 12 Rights of data subjects.
[147] Kuner, Christopher, Lee Bygrave, Christopher Docksey, and Laura Drechsler (n 143) p 67 – 69.
[148] Ibid.

The rights under the GDPR, Article 8 of the Charter of Fundamental Rights of the European Union (CFR) states:

'Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and based on the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right to access to data that has been collected concerning him or her, and the right to have it rectified. Compliance with these rules shall be subject to control by an independent authority.'

Everyone has the right to the privacy and personal data to be protected, processed in a fair and legal way, and accessible to the data subject anytime. Also, with the access to erasure or rectification. Under the Article 6 of the GDPR, the following sic conditions must accompany a lawful personal data process: Consent, Contract, For the organization to meet a legal obligation, Necessary for the protection of the vital interest of data subjects during data process, Necessary for the performance of public interest, Legitimate interest of the organization

European Data Protection Board (EDPB): The EDPB as a regulatory body is important in ensuring consistency of the GDPR principles and applications across the European Union and makes advisory services on issues concerning data protection.[149] It makes sure that update on the latest developments on data protection are effectively communicated within the stakeholders in EU, which makes the application of the GDPR comprehensive and effective. The key objective of its guidelines is for clarifications of the notions of the data controller and processor for consistency and harmonization of procedures with the EU area.[150]

News developments in data issues and regulations such as case laws from the courts are adequately updated and effected.

National Data Protection Authorities (DPAs): It ensures that GDPR compliance is enforced and addresses several complaints concerning data privacy. DPA's, data subject rights and the

[149] Kuner, Christopher, Lee Bygrave, Christopher Docksey, and Laura Drechsler (n 143) p 39.
[150] Ibid.

responsibilities of data controllers are keys to the EU data protection agenda. They act as guardians of consistency in the member states for the application of GDPR principles. [151]

A well functioning and independent DPAs is important in the EU data protection regulation. The NDAs makes data analyses comprehensible and applicable such as the court decisions of the Court of Justice of the European Union under the directive of the outdated Directive 95/46/EC It is important to safeguard personal data in a season when big data technological developments are put pacing the public authorities' regulatory applications.[152]

3.7. Conclusion

The European Convention on Human Rights remains one of the fundamental legal documents for the protection of human rights within Europe, with relevant mechanisms that impacts different sectors of human engagement such as the big data companies. Which recalls the ECHR objective of protecting and promoting the fundamental human rights and freedom within Europe. And a key standard for democracy, peace and justice.[153]

While it is the onus of big data companies and other data controllers to ensure that the process of data is in congruent with the basic principles under the ECHR and GDPR, it is an imperative for additional efforts to be made to ensure that the available legal framework and mechanisms are matching with the current technological developments that are reshaping our world.

In lieu of this, compliance with the ECHR provisions will require a multifaceted approach that is beyond the legal, regulatory and self- regulatory mechanisms by big data companies in lieu of the pace of technological developments and societal transformation. This rate of change will require a continuous dialogue with all stakeholders in data protection and the right to privacy, to ensure that the basic principles stated in the Convention will safeguard the individual rights in the information society and age.

[151] Giurgiu, Andra, and Tine A. Larsen (n 151) 342.
[152] Ibid.
[153] Monica Macovei 'A guide to the implementation of Article 10 of the European Convention on Human Rights' (Human Rights Handbook, No 2 2004).

The next chapters will look at future challenges and directions, evaluating the legal gaps and emerging technologies such as the artificial Intelligence and the future of the ECHR in the regulation of big data companies. A summary of key findings, recommendation and conclusion for policy makers and practitioners will be in the last chapter.

CHAPTER FOUR - Future Challenges and Directions

4.1. Introduction

Generally, it seems that emerging technologies are a source of hope because they are the engine of the digital era. This shift from the post-industrial period to the digital era where almost every sector of human endeavors is dependent on data for their survival and success adds to the notion of 'data paradigm shift'. This good news of technological innovations are also accompanied by new challenges we cannot ignore as individuals and as a society. There are legal challenges because of the interaction between technology and human rights.[154] This development must be based on a balanced approach to the use of technological innovations and the effects they create on the society.[155] There has been increasing cases on the breach of human rights by new technologies are on the rise at the European Court of Human Rights (ECtHR).[156] It becomes an imperative to consider the future challenges and directions related to the emerging technologies. Especially, the legal gaps that created the loopholes for big data companies to bypass the existing regulatory framework and mechanisms for data privacy and protection.

In witnessing the data paradigm shaping the world, and the rapid pace of change powered by innovative technological trends such as virtual reality (VR), artificial intelligence, the internet of things (IOT), blockchain technology, 3D printing, robotics and more. The advent of these technologies with the new social media is reshaping what it is meant to be human in the 21st century.[157] These challenges poses a threat to the fundamental principles of human rights, especially the right to privacy and data protection in the face of big data companies' race for the next innovation and the sovereignty of states. The emerging technologies, the influence of new digital media and new forms of discrimination is redefining our digital and social space. As we witness the emergence of multi digital identities made possible and permissible by technological features and cross border digital activities.[158]

[154] Van Dijk, P. and Van Hoof, G. J. H (n 154).
[155] Ibid.
[156] Ibid.
[157] Çöteli, Sami. 'The impact of new media on the forms of culture: digital identity and digital culture' (2019).
[158] Petryshyn, O. V., and O. S. Hyliaka (n 158) 15-23.

As these cutting-edge technologies converge to usher in a new digital era of information society that will impact every sector of our lives. The growing number of judgements at the ECtHR is a confirmation of a broader and ongoing assessment on the interface between technology and the provisions of the ECHR concerning the right to privacy and issues of data protection.[159]

The aim of this chapter is to identify the main legal issues with the regulatory authorities, courts and other mechanisms such as the ECHR as an instrument for the protection of fundamental rights. This chapter will look at the legal gaps and emerging technologies to mitigate their negative impact. Evaluate the future of the ECHR and big data regulations.

4.2. The Legal Gaps and Emerging Technologies

The current state of global economic development is characterized by the current advent of new technologies as the key drivers of the national and international growth and development.[160] As people's lives are continually reshaped in this digital world, it comes with different features of the exercise of rights and freedoms that requires a new set of norms that do not negatively impact the fundamental human rights.[161]

The growing legal gap between the new technologies and law is widening because the rate of technological developments are not on par with the legal mechanisms and regulatory bodies.[162] The sluggish response of legal and ethical oversight mechanisms are creating loopholes for big data companies to bypass existing legal framework for data protection and security. to meet up with the rate of changes in the digital era, public authorities are struggling to do away with outdated regulations and inadequate oversight.[163] This new effort will require the introduction of new legal frameworks and different approaches in an evolving technological landscape for an effective data governance and protection. Identified cause of the mismatch between the rate of technological development and legal oversights are the following:

[159] Van Dijk, P. and Van Hoof, G. J. H (n 154).
[160] Petryshyn, O. V., and O. S. Hyliaka. (n 158) 15-23.
[161] Ibid.
[162] Marchant, G.E 'The Growing Gap Between Emerging Technologies and the Law'. In: Marchant, G., Allenby, B., Herkert, J. (eds) The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight. The International Library of Ethics, Law and Technology, vol 7. (Springer, Dordrecht 2011) https://doi.org/10.1007/978-94-007-1356
[163] Ibid.

There are some legal problems that are overseen by obsolete public regulatory frameworks, which should be updated with the increasing technological developments. Supplementary legal mechanisms could be improved using the National Data Protection Authorities (NDAs) special powers in creating a harmonized and analyzed legal framework that are newly introduced from case laws, judicial reviews and legislations. NDA's plays a crucial role in the managements of data subject rights and the responsibilities of data controllers as keys to the EU data protection agenda. They act as guardians of consistency in the member states for the application of GDPR principles. [164] Another key problem is the lack of objective oversight. Solving problems needs proper identification and understanding of the issues.[165] Therefore, new legal instruments and approaches should be used to address new challenges of the emerging technologies. Addressing the gap between emerging technology and the law will require an outside the box methodology.[166]

Some of the regulatory gaps in regulating transformative technologies comes from unpredictable business models that outpaces the existing frameworks. The second gap is on data privacy and security, especially with the emergence of the AI. Lastly, is the AI analytical power. This conundrum where the AI makes its decision raises some ethical and legal concerns on how to ensure accountability and transparency of the AI system.

4.3. The Future of the ECHR and Big Data Regulation

It is important to know that even the good intentions of the ECHR to ensure that the original intent of the provision in protecting the basic principles of human rights within Europe, might not be enough to close the gaps. This is because of the conceptual failures in human rights provisions and application.[167] Also the good decisions of the ECtHR are not able to redress the conceptual errors could not do much.[168] Following an article, 'The European Convention on Human Rights, the EU and the UK: Confronting a Heresy' concluded in its fourth paper submission, on the ineffectiveness

[164] Giurgiu, Andra, and Tine A. Larsen 'Roles and Powers of National Data Protection Authorities: Moving from Directive 95/46/EC to the GDPR: Stronger and More' European' DPAs as Guardians of Consistency?' *Eur. Data Prot. L. Rev.* 2[2016] p 342.
[165] Marchant, G.E (n 162).
[166] Ibid.
[167] Stelios Andreadakis, The European Convention on Human Rights, the EU and the UK: Confronting a Heresy: A Reply to Andrew Williams, *European Journal of International Law* (Volume 24, Issue 4, November 2013) p 1187–1193, https://doi.org/10.1093/ejil/cht063
[168] Ibid.

of the courts procedural decisions aimed at redressing some conceptual flaws of the human rights regime.[169]

Andrew Williams was of the view of abandoning the ECHR and ECtHR regime because minor changes and updates through judicial reviews and case laws have proven to be futile. Rather, he proposed that the alternative should be expanded to avoid the systemin and conceptual flaws of the current regime.[170] Also, he argued that the present ECHR and ECtHR regime have limited benefits on the future of human rights. This is understandable in view of the pace of technological advances and the sluggish rate of regulatory reforms by government authorities to close the 'structural problems' that impedes good legal developments.[171]

Another challenge and future direction of big data and AI is on the recent progress and implications to education. Gaps in AI processing such as managing data privacy, fairness and optimizing educational outcomes should be addressed by redesigning the algorithmic models of the AI, addressing ethical issues of big data companies and other data controllers to improve personalized learning development.[172] The GDPR is a comprehensive legal mechanism that addresses data protection in the EU, but faces the challenges of cross-border data transfer and oversight. As data is global by nature, future should make provisions for adapting to the new technologies and data laws.[173] The global nature of data is a prerequisite for the adoption of a broader legal regime and framework that follows the principle of universalism. There is some sense in the adoption of the EU Charter instead of the Convention which is more advanced.[174] In terms of AI compatibility with the GDPR, it is important to know that AI was not explicitly mentioned in the GDPR.[175] Although, some GDPR provisions are relevant to AI applications with some challenges, on the new ways of data processing powered by AI. Issues of data limitation, minimalization, sensitive

[169] Ibid.
[170] Ibid.
[171] Ibid.
[172] Luan, Hui, Peter Geczy, Hollis Lai, Janice Gobert, Stephen JH Yang, Hiroaki Ogata, Jacky Baltes, Rodrigo Guerra, Ping Li, and Chin-Chung Tsai 'Challenges and future directions of big data and artificial intelligence in education' (Frontiers *in psychology* 2020).
[173] Mesarčík, M., Hamuľák, O 'General Data Protection Regulation: Current Challenges and Future Directions' In: Ramiro Troitiño, D. (eds) E-Governance in the European Union. Contributions to Political Science (Springer Cham 2024) https://doi.org/10.1007/978-3-031-56045-3_9.
[174] Williams, 'The European Convention on Human Rights, the EU and the UK: Confronting a Heresy', in this issue (2013) p 1165.
[175] Sartor, Giovanni, and Francesca Lagioia 'The impact of the General Data Protection Regulation (GDPR) on artificial intelligence' (2020) p 1-84.

data and making automated decisions with big data.[176] There should be a balanced approach on the data purpose between the input and output that enables economic development while protecting individual data.

In lieu of these, the European Court of Human rights (ECHR) is faced with challenge of adapting to today's digital world. The legal regime's structural problems that limits its effectiveness requires additional input that might include the expansion of its objective provisions that would address present legal issues such as the emergence of AI. The disruptive features of these technologies comes with legal and practical issues which are entirely different from previous ones prevalent at the time of the conception and drafting of the current legal framework and mechanisms we use. Aimed at closing the gaps that allows data controllers such as big data companies to bypass the current regulatory framework. It must redress issues related to data protection, surveillance, and rights to privacy by reshaping the current regulatory framework or crafting a new and effective regulations for big data usage.[177]

4.4. Conclusion

The evolution of new technologies should be followed by new legal mechanisms for oversight. Apparently, the ECHR is fundamental to the protection of individual data and the right to privacy within Europe. It has positive moral implications on human rights and democratic institutions in the geopolitical Europe and is seen as exemplary beyond the EU. However, navigating the transformative landscape of digital evolution would need a new authoritative framework, policies and protocols. A new regime that would reshape or replace the current mechanism should be inclusive, and human led with the capacity to use the full benefits of the evolving AI and big data.

This chapter explored the legal gaps and emerging technological changes that is affecting the regulating the application of data laws. It was identified that the pace at which emerging technologies are released to the public has disrupted the existing legal framework and regime. It was noted that this change is not balanced and has become a source of regulatory challenges.

[176] Ibid II.
[177] Teresa Rodríguez de las Heras Ballell 'Legal challenges of artificial intelligence: modelling the disruptive features of emerging technologies and assessing their possible legal impact' *Uniform Law Review* Volume 24 Issue 2, (2019) https://doi.org/10.1093/ulr/unz018 p 302–314.

Oversight becomes ineffective because of new features associated with new technologies. As a result, requires further legal expansion that accommodates new outcomes. This chapter identified the need to close the gap in the future by making a structural reform of the current legal regime, to adapt to new feature of new technologies and effective in protecting the right to privacy and individual data.

The next chapter is the last chapter for a summary of key findings of this study – assessing legal responsibilities and accountability mechanisms on big data companies through the ECHR. conclusions on this study will be summarized and recommendations made for further studies.

CHAPTER FIVE – Conclusion

5.1. Introduction

The original aim of this study was to assess the legal responsibilities and accountability mechanisms of big data companies through the European Convention on Human Rights. It was done to identify the problems and gaps in the existing legal frameworks for holding human rights violators accountable, analyse the current legal obligations under the ECHR and to assess the efficacy and application of the current accountability mechanisms under the ECHR. Also, offer recommendations to strengthen the legal and accountability mechanisms. The ECHR provides a comprehensive legal framework for assessing the legal responsibilities and accountability mechanisms of big data companies.[178] Providing certain rights and freedoms for the protection of individual data and the right to privacy.

In this chapter, I will summarise the key findings on this study, the contributions to the knowledge community and recommendations for further studies.

The purpose of this study is to investigate the existing legal obligations or responsibilities of data controllers, especially the big data companies within the context of the European Convention on Human Rights. As the pace of big data technological growth is faster than the rate of legal regulations to ensure the protection of the right to privacy and the right to the protection of personal data.

To facilitate this study and embark on this research the following research questions were framed:

1. What legal responsibilities do big data companies have on individual privacy rights?

2. How should ECHR be useful in the enforcement of these individual privacy rights?

3. What accountability mechanisms can be used to enforce compliance under the ECHR framework?

[178] Butin, Denis, and Daniel Le Metayer (n 10).

4. How do ECHR principles such as Article 6, Article 8 and Article 10 apply to big data companies processing personal data?

5.2. **Key Findings and Contributions**

This study evaluated some literatures on legal responsibilities of big data companies and accountability mechanisms under the ECHR and explored some case studies, reviews, and reports with some legal insights. While emphasising what the age of big data was commonly known for, in terms of collecting and analyzing vast proportion of personal information by companies.[179] It evaluated on effects the process of data has on the protection of individual rights and privacy. The study mentioned the importance of the current legal regime for assessing legal responsibilities and accountability of big data companies - the European Convention on Human Rights.[180]

The discussions on assessing legal responsibilities and accountability mechanisms evaluated the power of non-state and non-sovereign entities such as big data companies. These companies pose some features of sovereign states such as jurisdictional and extraterritorial influence which are within the framework and obligations of states.[181] And with global reach that complicates different jurisdictional legal frameworks for accountability and mechanisms, which is recipe for possible violations of human rights.[182] This comparative disadvantage exposes people to vulnerable situations where their data and privacy could be violated. If big data companies have been involved in the increasing cases of breach of privacy and data protection issues in developed states, it indicates troubling evidence of the under reported and unreported issues of breaches in developing states.

In acknowledgement of the recent advances in big data, artificial intelligence, and data-driven innovation, and benefits to the economic and societal transformation, it was clear that the dangers of unethical use of data would be unimaginable and could lead to the data processing bypassing

[179] Butin, Denis, and Daniel Le Metayer (n 10).
[180] Maghfirah, Fitri, and Fathayatul Husna 'CYBER CRIME AND PRIVACY RIGHT VIOLATION CASES OF ONLINE LOANS IN INDONESIA' In *PROCEEDINGS: Dirundeng International Conference on Islamic Studies* [2021] p 1-18.
[181] Ibid.
[182] Michalowski R.J and Kramer R.C. 'The Space Between Laws: The Problem of Corporate Crime in a Transnational Context' Social Problems (Oxford University Press, 1987) 34 (1) p 34 – 36.

the original intent of privacy and data protection law and ethical responsibility.[183] The 'datafication' process where devices capture, collect, store and process data in a cheaper, better and faster way could be usurped with huge implications to human rights.[184] A key issue experts noted was a 'corporate veil,' [185] that transnational corporations (TNCs) use in hiding their data operations, to avoid accountability for human rights violations. And benefitted from legal protection due to their legal personality, granting them special rights with opportunity to evade responsibilities.[186]

This study assessed the current gaps in the ECHR and identified areas that needs strengthening for legal responsibilities and accountabilities to be effective. Because Big data companies have a legal responsibility to protect consumers' data and adhere to regulations such as the General Data Protection Regulation.[187] Under the provisions of the ECHR, Big data companies must ensure to protect and respect individuals' rights and freedoms. While the ECHR provides a comprehensive legal framework for assessing the legal responsibilities and accountability mechanisms of big data companies.[188] It remains limited in applicability in some areas due to conceptual and structural issues.

In addition, it was realized that the time allocated for this study was not enough to dive into the wider scope of legal obligations and accountability frameworks, aimed for different objectives of data protection and activities. More mechanisms are crucial to this effect and urgently required as there has been an increasing rise in fake new, misinformation and disinformation. Big data companies need enhanced effort to close the loopholes of unethical and harmful uses of their platforms for public security.

---

[183] Bormida, Marina Da (n 2).
[184] Ibid.
[185] Ibid.
[186] Meeran R. 'The Unveiling of Transnational Corporations: A Direct Approach' in Addo M.K. (ed) 'Human Rights Standards and the Responsibility of Transnational Corporation' (The Hague: Kluwer Law International ,1999) p 161 – 170.

[187] Giakoumopoulos, C., G. Buttarelli, and M. O'Flaherty 'Handbook on European data protection law Luxembourg: Publications Office of the European Union, 2018) *https://doi. org/10.2811* 58814 2018.

[188] Butin, Denis, and Daniel Le Metayer (n 10).

The significance of this study is to find valuable insights on the legal responsibilities and accountability mechanisms on governing the operations of big data companies under the framework of the European Convention on Human Rights. And contribute to the existing body of knowledge through a comprehensive analysis on the legal responsibilities and accountability mechanisms on data companies, human rights, and the ECHR context. Which would be used in furthering academic discourse in fostering corporate accountability and responsibility on human rights issues for global data business operations. Informing policy makers, stakeholders and legal practitioners on the threats and opportunities of proportionality between the protection of human rights and advancement of technology.

Socio-legal research methodology, an interdisciplinary approach in legal analysis was used. It was vital in assessing and examining the intersection of law and the broader social contexts, helping to sum up the theoretical and empirical analysis through a combination of the perspectives and methodologies from legal and social sciences.[189] The data was acquired through primary sources such as reviews, court decisions and reports. Secondary data collection includes policy papers, academic reports and corporate social responsibility reports and books.

Following the discussions in the previous chapters, Chapter one emphasis was placed on the key concepts, definitions, literature review and analysis. The increasing role of big data companies in the global social, economic, and political order as it ushers in some challenges beyond borders. This chapter investigated how far the European Convention on Human Rights (ECHR) has gone as a legal framework for assessment and assurance of legal responsibilities and accountability mechanisms.

Chapter two presented the theoretical framework on big data, its nature, applications, and implications according to different terms of the evolution of the data. It evaluated the 'datafication' of the society, following the 'data paradigm' that influences behavioral changes for optimum and personalized alternatives. It went further with the application and implications of big data, with the ethical, and legal aspects for privacy and data protection. Also explored who big data impacts human rights, such as the right to privacy and the right to data protection.

[189] Johansen, Stian Oby '*The human rights accountability mechanisms of international organizations*' (Cambridge University Press, 2020).

Chapter three explored the key principles of the ECHR in enforcing obligations and accountability on big data companies. The relationship between the privacy rights, the scope of the freedom of expressions and the right to effective remedy were elaborated. There were separate accountability mechanisms companies could initiate as part of the mandate to ensure ethical data process of data, and respect for the rights to privacy. The role and authority of regulatory bodies are vital to data protection and one of the centers of the European regulatory centers for the protection of the right to privacy within Europe.

Chapter four evaluated some legal challenges based on the interaction between technology and human rights.[190] And emphasized on that the development should be a balanced approach for technological innovations and human rights of the society.[191] An increasing rate of cases on the breach of human rights by new technologies at the European Court of Human Rights (ECtHR) raise some concerns.[192] This makes it important to consider the future challenges and directions related to the emerging technologies. This chapter identified the main legal issues with the regulatory authorities, courts and other mechanisms. And the legal gaps that needs to be closed to mitigate the negative impacts of emerging technologies.

Chapter five of this study examined the scope of the legal framework regime and its efficacy through the summary of the key findings of the previous chapters, the contributions and recommendations for further studies.

In consideration of the legal responsibility and accountability mechanisms of big data companies, within the current ECHR and ECtHR regime, the following inferences can be made with regards to the main research questions and sub-questions:

What legal responsibilities do big data companies have on individual privacy rights?

Apart from many national and regional laws that regulates big data companies within the EU, the GDPR and the ECHR provisions are critical to the right to privacy and data protection. Big data

[190] Van Dijk, P. and Van Hoof, G. J. H (n 159).
[191] Ibid.
[192] Ibid.

companies have the responsibility to ensure that collected data, processed, and disseminated will not breach the right to privacy. Key responsibilities include the right to privacy (Article 8), ensuring the right to the freedom of expression (Article 10), and making sure that there is effective remedies if any of these rights are violated (Article 13).

Among five EU regulations and directives on data protection, with different objectives.[193] This study identified the ECHR as the key legal framework apart from the GDPR on being instrumental on individual privacy rights and data protection. The scope of Article 8 of the ECHR includes that of personal data and private life. According to the ECtHR, it is necessary to protect the individual from any form of intrusion to their privacy from state and non - state agents such as the big data companies. It is the onus of companies to adhere to their obligatory duties and ethics to ensure that effective privacy and data protection are guaranteed.[194] However, restrictions of the right under Article 8 of the ECHR are imposed on certain conditions that permits the public authorities to interfere with the right to private and family life, home and correspondence. Interference is allowed within the context of certain actions that are considered lawful, necessary and proportional under the law to protect the following: National security, public safety purposes, The economy, Health or morals, The rights and freedoms of others, and prevent crime or disorder in the society.

How should ECHR be useful in the enforcement of these individual privacy rights?

There are many ways to hold big data companies accountable through a mix of legal, regulatory and independent company ethical mechanisms.

Under the ECHR, Article 8, the right to private and family life protects the individual privacy and their family life, home and correspondence from arbitrary interference by the government or any other public authorities. The European Court of Human Rights based at Strasbourg, France, comes into the rescue, when national legal remedies have been exhausted. The ECtHR ensures that the provisions under the ECHR are implemented for the member states. Individuals can approach this

[193] Lenz, Rainer ‘Big Data (n 108)19.
[194] Guide on Article 8 of the European Convention on Human Rights “Right to Respect for Private and Family Life” (European Court of Human Rights, 2024) p 7.

court with cases that could not be redressed at their national courts.[195] The national courts and ECtHR mechanism allows judicial process where individuals whose rights and freedoms under the provisions of the ECHR have been violated, could possibly seek redress. Articles 13 of the ECHR ensures the efficacy of this legal mechanism.[196]

In lieu of this, big data companies are obligated to ensure that individuals have access to address their grievances with regards to any of the provisions of the ECHR, such as breach of the right to privacy, complaints on lack of transparency and efficacy of the regulatory agencies.[197] The objective of Article 13 is to ensure that individual's whose Convention rights have been breached, could get relief from their national jurisdictions, before seeking a redress from the international court, which is the ECtHR. In other words, the primary responsibility to the protection of the Conventions rights is the onus of the member states.[198]

What accountability mechanisms can be used to enforce compliance under the ECHR framework?

A mix of accountability mechanisms includes legal, regulatory and independent company's ethical mechanisms. The legal mechanisms includes the national courts and ECtHR mechanism which allows judicial process where individuals whose rights and freedoms under the provisions of the ECHR have been violated, could seek redress under the Article 13 of the ECHR.[199] The national courts are the first point of call for the defense of rights and freedoms for the right of privacy. Redress is done within the national courts where both national and incorporated international human rights norms could be applied.[200] Following the national courts is the European Court of Human Rights based at Strasbourg, France, which comes into the rescue, when the national legal remedies have been exhausted. The ECtHR ensures that the provisions under the ECHR are

[195] Laurence R. Helfer 'Redesigning the European Court of Human Rights: Embeddedness as a Deep Structural Principle of the European Human Rights Regime' (*European Journal of International Law* Volume 19 Issue 1 2008) p 125–159, https://doi.org/10.1093/ejil/chn004 .
[196] Marko Bošnjak, Kacper Zajac 'Judicial Activism and Judge-Made Law at the ECtHR' (*Human Rights Law Review* Volume 23 Issue 3 2023) Available at https://doi.org/10.1093/hrlr/ngad015.
[197] Council of Europe: European Court of Human Rights, *Guide on Article 13 of the European Convention on Human Rights - Right to an Effective Remedy* (2020) p 84.
[198] Kudla vs Poland [GC] 2000 & 152.
[199] Marko Bošnjak, Kacper Zajac 'Judicial Activism and Judge-Made Law at the ECtHR' (*Human Rights Law Review* Volume 23 Issue 3, 2023) Available at https://doi.org/10.1093/hrlr/ngad015.
[200] Ibid.

implemented for the member states. Individuals can approach this court with cases that could not be redressed at their national courts.[201] Other regulatory mechanisms are important in ensuring the right to privacy and data protection are applied in different jurisdictions. European member states Data Protection Authorities (DPA's) whose primary responsibility is to enforce compliance of the data protection laws such as the General data Protection Regulation (GDPR) and other key provisions of privacy rights under the ECHR.[202] The DPA's ensure that big data companies and other data controllers comply with the legal requirements of the existing legal mechanism.[203] The Article 8 of the ECHR plays a crucial role in interpreting and enforcing data protection norms, because of its provisions for the right to respect private and family life.

How do ECHR principles such as Article 6, Article 8 and Article 10 apply to big data companies processing personal data?

Under the ECHR, the fundamental provisions for the right to privacy and data protection are the Article 6: The right to a fair trial ensures the right to a fair and public hearing by an independent and impartial tribunal set up according to the law within a reasonable period. Big data companies must ensure that their data process adheres to the acceptable standards such as transparent, lawful, and fair. This includes that data subjects are provided a clear information on how their data is processed, and any information on big data analytics that complies with the law.[204]

Article 8: The right to private and family life protects the individual privacy and their family life, home and correspondence from arbitrary interference by the government or any other public authorities. Big data companies must respect individuals' privacy when processing personal data.

And the Article 10: The freedom of expression guarantees the right to the freedom of expression, which includes holding personal opinions and receiving or impact information and ideas without

[201] Laurence R. Helfer 'Redesigning the European Court of Human Rights: Embeddedness as a Deep Structural Principle of the European Human Rights Regime' (*European Journal of International Law* Volume 19 Issue 1 2008) p 125–159, https://doi.org/10.1093/ejil/chn004 .
[202] Guide on Article 8 of the European on Human Rights ' Right to Respect for Private and Family Life' (European Court of Human Right 2024) p 7 https://rm.coe.int/guide-on-article-8-of-the-european-convention-on-human-rights/16808e67cb
[203] Case-Law of the European Court of Human Rights Data Protection. https://rm.coe.int/guide-on-article-8-of-the-european-convention-on-human-rights/16808e67cb
[204] Guide to the Case-Law of the European Court of Human Rights Data Protection [2024] Guide to the Case-Law - Data protection (coe.int).

the interference of the public authority. This right correlates with data processing and big data companies must balance their data driven goals and human rights requirements.

These ECHR principles are key to the ethical and legal aspects of data processing that shows the society's interest and individual rights. So, following the GDPR guide will be helpful for big data companies to navigate through the challenges of the digital era.

5.3. Recommendations

One can conclude that assessing legal responsibilities and accountability mechanisms of big data companies through the ECHR in important to further academic discourse and foster corporate accountability and responsibility on human rights issues for global data business operations. Informing policy makers, stakeholders and legal practitioners on the threats and opportunities of big data and human rights. Based on the above discussions and responses:

It is recommended that to have a general definition of personal data which will be crucial in creating a more comprehensive sets of legal norms for effective application. The definition of personal data under the GDPR as being static does not match with the reality of the emerging nature of personal data as the nature of data is gradually changing; its static form poses a challenge for the 'GDPR compliancy' in a dynamic digital era.

The second recommendation is to have a general definition of personal data which will be crucial in creating a more comprehensive sets of legal norms for effective application. The definition of personal data under the GDPR as being static does not match with the reality of the emerging nature of personal data. As the nature of data is gradually changing; its static form poses a challenge for the 'GDPR compliancy' in a dynamic digital era.

The third recommendation to look at some ethical issues that could raise tensions about the right to privacy because the use of big data analytics poses a great risk to privacy when the technique of data collection and analysis are done without the consent or understanding of the data subjects. Improved ethical checks will improve the lack of control and transparency and minimize the impacts on privacy rights.

The fourth recommendation is to develop special human rights guidelines for big data analytics to ensure integrity in data monitoring and informed activism because the data analytics raise ethical issues, when state and non-state agencies perform inappropriate surveillance on people. This ethical dilemma is a breach of the right to privacy.

The fifth recommendation is to use a socio-legal methodology approach in solving this complex issue to rephrase the concept of privacy in data protection, in congruent with the provisions of the ECHR. A viable solution must be multidisciplinary, involving technological, ethical and legal perspectives. This is useful for clearer legal objectives and concept that can address the vital aspects of the legal scope required for creating the structural changes and effective outcomes. Updated legal versions should focus on the emerging technologies such as the artificial intelligence (AI), robotics and others, to ensure that there is adequate measure in place to curb unwanted consequences that could breach the fundamental principles of human.

The sixth recommendation is to expand the legal scope to redefine the legal personality of transnational corporations (TNCs). TNCs such as big data companies are increasingly becoming crucial in international development and cooperation. And are financially richer than many member states, their operations involve people and occupies territories. While companies are not sovereign states but are really exercising some of the characteristics of sovereign states such as jurisdictional and extraterritorial influence which are within the framework and obligations of states. The pace of geographic and economic expansion adds to their extra-territoriality, with benefits to escape accountability in states with smaller and weaker legal regimes and authorities. The ECHR with a broader and geopolitical legal authority with Europe can adopt the principle of universalism with global impact for human rights.

Conclusion

This study involved a multifaceted analytical approach on assessing the legal responsibilities and accountability mechanism within the context of the ECHR framework. It also evaluated the connection between the ECHR and GDPR on laying the foundation for the EU data protection agenda and for ethical corporate activities. The conclusion emphasises on the interplay between ethics, law, and big data accountability. And the need for developing key guidelines for big data

companies to ensure the protection of human rights and personal data. Having provided the contribution of this study, summary of key findings and recommendations. This research has thoroughly investigated the legal responsibilities and accountability mechanisms of big data companies under the ECHR framework.

6. Bibliography

6.1. Primary sources

6.1.1. Legislation, Texts, and Statutes

Article 8 of the ECHR 'Respect for your private and family life' Equality and Human Rights Commission EHRC [2021] Available at equalityhumanrights.com [Accessed July 20, 2024].

Article 10 of the ECHR 'Freedom of Expression' Equality and Human Rights Commission EHRC [2021] Available at equalityhumanrights.com [Accessed July 20, 2024].

Case-Law of the European Court of Human Rights Data Protection Available at https://rm.coe.int/

Council of Europe: European Court of Human Rights Guide on Article 13 of the European Convention on Human Rights - Right to an Effective Remedy [2020] p 84.

GDPR 'REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL' of 27 April 2016 on the protection of natural persons regarding the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Guide on Article 8 of the European on Human Rights 'Right to Respect for Private and Family Life' European Court of Human Right [2024] https://rm.coe.int/ p 7.

European Convention on Human Rights (ECHR) Article 10 > Accessed https://www.echr.coe.int/documents/d/echr/guide_art_10_eng > 8 November 2023.

UN General Assembly Universal Declaration of Human Rights (UDHR) (1948 217 A III) > Accessed 10 November 2023.

6.1.2. Case laws

Kudla vs Poland [GC] [2000] 152.
S. and Marper v. The United Kingdom [2008] 30562/04 and 30566/04.

6.2. Secondary Sources

6.2.1. Books and Articles

Acharjya, Debi Prasanna, and Kauser Ahmed. 'A survey on big data analytics: challenges, open research issues and tools' *International Journal of Advanced Computer Science and Applications* 7.2 (2016) 511-518.

Bormida, Marina Da 'The big data world: Benefits, threats and ethical challenges' In *Ethical Issues in Covert, Security and Surveillance Research* (Emerald Publishing Limited, 2021) p 71 -91.

Butin, Denis, and Daniel Le Métayer ‘A guide to end-to-end privacy accountability’ In *2015 IEEE/ACM 1st International Workshop on Technical and Legal aspects of data privacy and Security* (2015) p20-25 IEEE.

Bryant, Randal E ‘Data-intensive scalable computing for scientific applications’ (*Computing in Science & Engineering* 13.6, 2011) p 25-33.

Chenthara, Shekha, Hua Wang, and Khandakar Ahmed ‘Security and privacy in big data environment’ (2018).

Çöteli, Sami ‘The impact of new media on the forms of culture: digital identity and digital culture’ (2019).

Couldry, N., & Mejias, U. A ‘Data Colonialism: Rethinking Big Data’s Relation to the Contemporary Subject’ (Television & New Media, 20(4) 2019) p 336-349. https://doi.org/10.1177/1527476418796632

Cumbley and Church ‘Is “Big Data” creepy?’ (Computer Law & Security Review, 29, 2013) p 601–609.

Davenport, Thomas H., and Jill Dyché ‘Big data in big companies’ *International Institute for Analytics* 3, no. 1-31 (2013).

Devins, Caryn, Teppo Felin, Stuart Kauffman, and Roger Koppl. ‘The law and big data’ *Cornell JL & Public Policy* 27, 357. 2017) p 360.

Douglas Laney ‘3d data management: Controlling data volume, velocity and variety’ Gartner [2001]: 02-06.

European Economic and Social Committee ‘The ethics of big data: balancing economic benefits and ethical questions of big data in the EU policy context’ *European Union* [2017] p. 36.

Floridi, Luciano ‘The fourth revolution: How the infosphere is reshaping human reality’. OUP Oxford [2014].

Gasser, Urs, and Virgilio AF Almeida ‘A layered model for AI governance’ (IEEE Internet Computing 21 no 6, 2017) p 58-62.

Geoffrey West ‘Big Data Needs a Big Theory to Go with it’ SCI. AM (2013) Available at https://www.scientificamerican.com/ article/big-data-needs-big-theory/ Accessed 12 May 2024.

Gianclaudio Malgieri ‘Automated decision-making in the EU Member States: The right to explanation and other “suitable safeguards” in the national legislations’ (Computer Law & Security Review, 2019) Volume 35, Issue 5,105327, ISSN 0267-3649 https://doi.org/10.1016/j.clsr.2019.05.002.

Giakoumopoulos, C., G. Buttarelli, and M. O’Flaherty ‘Handbook on European data protection law’ (Luxembourg: Publications Office of the European Union, 2018) https://doi. org/10.2811 58814.

Giurgiu, Andra, and Tine A. Larsen 'Roles and Powers of National Data Protection Authorities: Moving from Directive 95/46/EC to the GDPR: Stronger and More' European' DPAs as Guardians of Consistency?' *Eur. Data Prot. L. Rev.* 2 (2016) p 342.

Goodman, Bryce, and Seth Flaxman 'European Union regulations on algorithmic decision-making and a "right to explanation' (*AI Magazine* 38, no 3, 2017) p 50-57.

Hale, Sandra 'The discourse of court interpreting' (2004) p 1-288.

Hashem, Ibrahim Abaker Targio, et al. 'The rise of "big data' on cloud computing: Review and open research issues.' (*Information systems* 47, 2015) p 98-115.
Harvard Law Review 'Developments in the Law – Criminal Law Part V: Corporate Liability for Violations of International Human Rights Law' (Vol 114 No 7, 2001) p 2025 – 2048.

Ishikiriyama, Célia Satiko and Carlos Francisco Simões Gomes. 'Big Data: A Global Overview' Studies in Big Data (2018).

Johansen, Stian Oby 'The human rights accountability mechanisms of international organizations' (Cambridge University Press, 2020).

Karthik Kambatlaa, Giorgos Kollias b, Vipin Kumarc, Ananth Gramaa, Trends in big data Analytics, (2014) 74 2561–2573

Katal, Avita, Mohammad Wazid, and Rayan H. Goudar 'Big data: issues, challenges, tools and good practices' Sixth *international conference on contemporary computing* (IC3) (IEEE, 2013).

Khoury S. Transnational corporations and the European Court of Human Rights: Reflexions on the Indirect and Direct Approaches to Accountability. Sortuz: (Oñati Journal of Emergent Socio-Legal Studies. 2010) 4(1) p 69.

Kim, Gang-Hoon, Silvana Trimi, and Ji-Hyong Chung 'Big-data applications in the government sector' *Communications of the ACM* 57.3 (2014) p78-85.

Kuner, Christopher, Lee Bygrave, Christopher Docksey, and Laura Drechsler '*The EU general data protection regulation: a commentary'* (Oxford University Press, 2020) Available at: https://globaloup.com/academic.

Laurence R. Helfer 'Redesigning the European Court of Human Rights: Embeddedness as a Deep Structural Principle of the European Human Rights Regime' *European Journal of International Law* Volume 19 Issue 1, 2008) https://doi.org/10.1093/ejil/chn004 p 125 - 159.

Lenz, Rainer 'Big Data: Ethics and Law' (SSRN Electronic Journal, 2019) 10.2139/ssrn.3459004 p 15.

Lokshina, Izabella V., and Cees JM Lanting 'Addressing ethical concerns of big data as a prerequisite for a sustainable big data industry' *International Journal of Interdisciplinary Telecommunications and Networking (IJITN)* 10, no 3, 2018) p 33-54.

Luan, Hui, Peter Geczy, Hollis Lai, Janice Gobert, Stephen JH Yang, Hiroaki Ogata, Jacky Baltes, Rodrigo Guerra, Ping Li, and Chin-Chung Tsai 'Challenges and future directions of big data and artificial intelligence in education' (Frontiers *in psychology,* 11 2020) 580820.

Mahmoudian, Mahshad & Zanjani, s. Mohammadali & Shahinzadeh, Hossein & Kabalci, Yasin & Kabalcı, Ersan & Ebrahimi, Farshad 'An Overview of Big Data Concepts, Methods, and Analytics: Challenges, Issues, and Opportunities (2023) 10.1109/GPECOM58364.2023.10175760.

Maghfirah, Fitri, and Fathayatul Husna 'CYBER CRIME AND PRIVACY RIGHT VIOLATION CASES OF ONLINE LOANS IN INDONESIA' In *PROCEEDINGS: (*Dirundeng International Conference on Islamic Studies, 2021) p 1-18.

Manyika, James, Michael Chui, Brad Brown, Jacques Bughin, Richard Dobbs, Charles Roxburgh, and Angela Hung Byers 'Big data: The next frontier for innovation, competition, and productivity' (2011).

Mark Graham, Big Data and the End of Theory? THE GUARDIAN (2012), available at https://www.theguardian.com/news/datablog/2012/mar/09/big-data-theory accessed 12 May 2024.

Marchant, G.E 'The Growing Gap Between Emerging Technologies and the Law'. In: Marchant, G Allenby, B., Herkert, J (eds) 'The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight' The International Library of Ethics, Law and Technology vol 7 (Springer Dordrecht, 2011) https://doi.org/10.1007/978-94-007-1356.

Meeran R. 'The Unveiling of Transnational Corporations: A Direct Approach' in Addo M.K. (ed) 'Human Rights Standards and the Responsibility of Transnational Corporation' (The Hague: Kluwer Law International, 1999) p 161 – 170.

Mesarčík, M., Hamuľák, O 'General Data Protection Regulation: Current Challenges and Future Directions' In: Ramiro Troitiño, D. (eds) E-Governance in the European Union. Contributions to Political Science Springer Cham (2024) https://doi.org/10.1007/978-3-031-56045-3_9.

Michalowski R.J and Kramer R.C. 'The Space Between Laws: The Problem of Corporate Crime in a Transnational Context' Social Problems (Oxford University Press,1987) 34 (1) p 34 – 36.

McNeely, Connie L., and Jong-on Hahm 'The big (data) bang: Policy, prospects, and challenges' *Review of Policy Research* 31, no 4 (2014) p 304-310.

Mayer-Schönberger, Viktor, and Kenneth Cukier '*Big data: A revolution that will transform how we live, work, and think*' (Houghton Mifflin Harcourt, 2013).

Miron-Shatz, T., A. Y. S. Lau, C. Paton, and M. M. Hansen 'Big data in science and healthcare: A review of recent literature and perspectives' *Yearbook of Medical Informatics* 23, no. 01, 2014) p 21-26.

Monica Macovei 'A guide to the implementation of Article 10 of the European Convention on Human Rights' (Human Rights Handbook No 2, (2004).

Nersessian, David ‘The law and ethics of big data analytics: A new role for international human rights in the search for global standards’ (Business Horizons 61 no 6, 2018) p 845-854.

Neelam Singh, Neha Garg, Varsha Mittal ‘Data – insights, motivation and challenges’ (Volume 4, Issue 12, 2013) 2172, ISSN 2229-5518.

O'Donnell, Thomas A ‘The margin of appreciation doctrine: standards in the jurisprudence of the European Court of Human Rights’ (Hum. Rts. Q. 4 1982) p 474.

Oussous, Ahmed, et al. ‘Big Data technologies: A survey’ *Journal of King Saud University*-(Computer and Information Sciences 30.4 2018) p 431-448.

Perera, Charith, et al. ‘A survey on internet of things from industrial market perspective’ *IEEE Access* 2 [2014]: 1660-1679.

Peter Fitzpatrick and Hunt Alan ‘Introduction” Journal of Law and Society' [1987] 14(1) p 1 JSTOR > https://doi.org/10.2307/1410292 > Accessed 18 November 2023.

Petryshyn, O. V., and O. S. Hyliaka ‘Human rights in the digital age: Challenges, threats and prospects’ 28 no 1 (2021) p 15-23.

Politou, Eugenia, Efthimios Alepis, and Constantinos Patsakis. ‘Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions’ (Journal of cybersecurity 4, no 1, 2018) 01.

Price, W. Nicholson, and I. Glenn Cohen ‘Privacy in the age of medical big data’ *Nature medicine* 25, no. 1 2019) p 37-43.

Qiu, J., Wu, Q., Ding, G. *et al.* ‘A survey of machine learning for big data processing. *EURASIP J. Adv. Signal Process’* (2016) p 67 https://doi.org/10.1186/s13634-016-0355-x

Roger Koppl et al. ‘Economics for a Creative World’ 11 J. INSTITUTIONAL ECON. 1, 4 (2013).

Smid, Miles E., and Dennis K. Branstad ‘Data encryption standard: past and future’ *Proceedings of the IEEE* 76.5 (1988) p 550-559.

Sartor, Giovanni, and Francesca Lagioia ‘The impact of the General Data Protection Regulation (GDPR) on artificial intelligence’ [2020] p 1-84 Steiner H.J. et al International Human Rights in Context: Law, Politics, Morals (3rd ed Oxford University Press, 2008) p 1388.

Szalay, Alex ‘Extreme data-intensive scientific computing’ *Computing in Science & Engineering* 13.6 (2011) p 34-41.

Stelios Andreadakis, ‘The European Convention on Human Rights, the EU and the UK: Confronting a Heresy: A Reply to Andrew Williams’ *European Journal of International Law*, (Volume 24 Issue 4 ,2013) p 1187 - 1193, https://doi.org/10.1093/ejil/cht063.

Teresa Rodríguez de las Heras Ballell ‘Legal challenges of artificial intelligence: modelling the disruptive features of emerging technologies and assessing their possible legal impact’ (Uniform Law Review Volume 24 Issue 2. 2019) p 302 - 314 https://doi.org/10.1093/ulr/unz018.

Tucker ‘Has Big Data made anonymity impossible?’ In: Big Data gets personal (MIT Technology Review, 2013).

Van der Sloot, B., & Van Schendel, S ‘Ten questions for future regulation of big data: A comparative and empirical legal study’ (J Intel Prop Info Tech & Elec Com 2016) L7 p 110.

Van Dijk, Pieter, and Godefridus JH Van Hoof. *Theory and practice of the European Convention on Human Rights* (Martinus Nijhoff Publishers, 2023) p 1.

Vijayarani, S., and S. Sharmila ‘Research in big data: an overview’ (Inf Eng Int J 4, 2016) p 1-20.

Wachter, S., & Mittelstadt, B ‘A right to reasonable inferences: re-thinking data protection law in the age of big data and AI’ (Columbia Business Law Review, 2019).

Williams, ‘The European Convention on Human Rights, the EU and the UK: Confronting a Heresy’ in this issue (2013) p 1165.

Zhang Dongpo ‘Big data security and privacy protection’ *8th international conference on management and computer science* (ICMCS Atlantis Press, 2018).

Zlobina A ‘Human Rights Obligations of Information and Communication Technology Companies in the Context of Data Governance’ [Dissertation] University of Nottingham A.Y. [2017/2018] p 5.

6.2.2. Report and policy papers.

6.2.3. Appendices

Figure 1 – Big Data Figure

Vijayarani, S., and S. Sharmila ‘*Research in big data: an overview’* Inf Eng Int J 4 [2016] p 2.