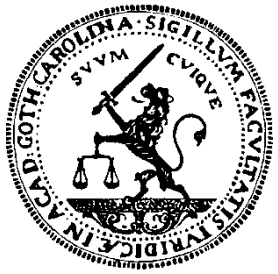

FACULTY OF LAW
Lund University

Ieva Vaitkunaite

Reinventing the Right to Privacy Towards Full-Fledged Informational Self-Determination

A doctrinal study of the evolutive interpretation of Article 17 of ICCPR

JAMM07 Master Thesis

International Human Rights Law
30 higher education credits

Supervisor: Ana Nordberg

Term: Spring 2023

SUMMARY

The right to privacy, as enshrined in the International Covenant on Civil and Political Rights, was developed at a time predating the digital revolution. In order to adapt this right to the technological advancements of the digital age, international organisations like the UN have sought methods of interpretation that accommodate these new circumstances. One such method is evolutive interpretation, which approaches the right to privacy as a living instrument and interprets it in the light of new circumstances. While evolutive interpretation has undeniable advantages, the thesis argues that it alone is insufficient for upholding the right to privacy in the digital age. Solely applying the right to privacy to new circumstances without comprehensive legal reform exacerbates the fragmentation between the two legal frameworks – privacy and data protection – ultimately failing to ensure informational self-determination sufficiently.

Unlike most legal studies, the thesis delves beyond the normative aspects of privacy and links it to informational self-determination. In the modern age, informational self-determination has gained increasing significance for individuals. It encompasses aspects of privacy and data protection and is rooted in the fundamental principle of human dignity. To demonstrate how modern technologies undermine the boundaries of informational self-determination, the thesis "confronts" the right to privacy with practical challenges posed by Big Data analytics. As a result, the work addresses a significant gap in international law, that of neglecting the division between privacy and data protection. It sets forth a new approach: the right to data protection as a distinct human right next to privacy.

PREFACE

This work is dedicated to my mother. An endless source of love, support, and inspiration in my life. You have always been the driving force behind my pursuit of knowledge.

This thesis also culminates two years of studying international human rights law. It is a testament to the transformative journey that has taken place within me. As I traversed through the complex territory of international human rights law, I realised that mere articulation of problems is insufficient. We must also strive to be agents of change, seeking tangible solutions to profound human rights challenges.

To the community of the faculty of law, I cannot thank you enough for your guidance, encouragement, and motivation.

TABLE OF CONTENTS

TABLE OF FIGURES

ABBREVIATIONS

CFREU	Charter of Fundamental Rights of the European Union
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
ICCPR	International Covenant on Civil and Political Rights
ICJ	International Court of Justice
VCLT	Vienna Convention on the Law of Treaties

1. INTRODUCTION

1.1. Background

Years of limited regulation of the digital environment have led to the privacy paradox: people believe they are protected from privacy threats, yet in their behaviour, they relinquish personal data for very little in exchange or fail to use measures to protect their privacy. As billions of people worldwide use the internet as their primary mode of conducting their private and professional affairs, they are exposed to Big Data induced privacy threats daily. Big Data processing tools have facilitated privacy intrusions and made such violations seamless. While these tools represent a paradigm shift in collecting, processing, and analysing information, they have significant negative consequences on human rights, especially the right to privacy.

Traditionally, discussions about the right to privacy are limited to the scope of the 1948 Universal Declaration of Human Rights[1] and the 1966 International Covenant on Civil and Political Rights[2] (ICCPR). It is a rather simplistic approach and does not reveal the nuances related to this right. Therefore, the thesis builds upon four core concepts: privacy, data protection, evolutive interpretation, and informational self-determination.

Regarding privacy, Article 17 of the ICCPR protects everyone from arbitrary or unlawful interferences with their "privacy, family, home or correspondence."[3] This right was articulated in the pre-internet times before new information technologies emerged. In order to sustain its relevance in the changing digital environment and address new-age privacy threats, human rights tribunals and the UN human rights treaty bodies employed evolutive interpretation to adapt the right to present-day conditions without the need to amend the treaty formally. However, the question is whether this approach is enough to ensure a robust international privacy framework and informational self-determination.

The concept of informational self-determination is of utmost importance in the digital age. In 1983, the German Federal Constitutional Court[4] first developed this concept, which later spread to other legal systems including the Council of Europe. Informational self-determination encapsulates a notion of "the authority of the individual

[1] UN General Assembly, *Universal Declaration of Human Rights*, Resolution 217 A (III), 1948.
[2] UN General Assembly, International Covenant on Civil and Political Rights (1966) Treaty Series 999.
[3] Ibid., Art. 17(1).
[4] German Federal Constitutional Court, *Order of the First Senate* (1983) 1 BvR 209/83.

to decide himself or herself, based on the idea of self-determination, when and within what limits information about his or her private life should be communicated to others."[5] This concept connects privacy to the highest principle of human dignity as well as it highlights individual autonomy over personal data and the contextual integrity of that information. In the digital age context, the thesis aims to demonstrate how Big Data analytics undermines informational self-determination and expose the neglected problem in international privacy law – the fragmentation between privacy and data protection.

Privacy and data protection are the cornerstones of international privacy law. Each of these regimes has its scope, goals, and application. However, they enjoy different levels of recognition at the international level. International law recognises the right to privacy as a human right in numerous international treaties and instruments, including the Universal Declaration of Human Rights[6] and the ICCPR.[7] Data protection is not a freestanding human right, according to the ICCPR. However, the UN Human Rights Committee has stated in the UN General Comment 16 that Article 17 requires legal implementation of essential data protection guarantees in both the public and private sectors.[8] The lack of international recognition of data protection has led to disintegration of international privacy law, confusion, inconsistency, and gaps in legal interpretation.

Therefore, the hypothesis of the thesis is that the evolutive interpretation of the right to privacy leads to the more profound fragmentation between privacy and data protection, increasing the erosion of the boundaries of informational self-determination. In addition, technological developments have a magnifying effect – they enhance the gaps in international privacy law. The problem has a tremendous impact on the privacy of billions of people. It is, thus, necessary to consider alternative approaches to repair the overlap between privacy and data protection, as well as introduce a comprehensive legal reform, i.e., to recognise data protection as a freestanding human right.

---

[5] Rouvroy A and Poullet Y. The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy. In Gutwirth S et al. (eds.), *Reinventing Data Protection?* Springer, Dordrecht, 2009, 45.

[6] UN General Assembly, *Universal Declaration of Human Rights*, Resolution 217 A (III), 1948, Art. 12.

[7] UN General Assembly, International Covenant on Civil and Political Rights (1966) Treaty Series 999, Art. 17.

[8] UN Human Rights Committee, *CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation,* 1988., paras 7 and 10.

1.2. Prior Research

A systematic literature review of existing research identified "key information relevant to the topic"[9] in two legal databases, Oxford Academic and LUBsearch. While there are many other databases, the thesis utilised those available for the students at Lund University. The search terms included "Big Data," "international human rights law," and "privacy".

Several legal books and journals, including the International Data Privacy Law and the International Journal of Law and Information Technology published fifteen legal studies that met the inclusion criteria. The studies covered various topics related to Big Data and international law, for example, the right to privacy, non-discrimination, and accountability. However, more recent studies demonstrated a gradual shift in focus towards the right to privacy. The studies identified in this review highlight the potential impact of Big Data analytics on the right to privacy, particularly in surveillance, data protection, and algorithmic decision-making.[10]

The outcomes of the systematic literature review reveal five key issues. Firstly, the vague scope of Article 17 of ICCPR.[11] Secondly, a tendency to deal with the right to data protection as an expression of the right to privacy.[12] Thirdly, creating detailed profiles by gathering massive amounts of personal data that provide more information about individuals than they may know about themselves.[13] Fourthly, questionable adaptability of current international privacy law standards to the constantly evolving digital environment.[14] Fifthly, fragmentation, polarisation, and hybridisation in digital governance.[15] The findings confirm the elusive meaning of the right to privacy under Article 17 of the ICCPR. Accordingly, privacy concerns are often vague and ill-formed,

[9] Ishwara PB. *Idea and Methods of Legal Research*. Oxford University Press, 2019, 116.
[10] See, e.g., Kinfe Y. *Privacy and the Role of International Law in the Digital Age*. Oxford University Press, 2023; Land KM and Aronson DJ (eds.). *New Technologies for Human Rights Law and Practice*. Cambridge University Press, 2018.
[11] Kinfe Y. *Privacy and the Role of International Law in the Digital Age*. Oxford University Press, 2023, 33.
[12] See, e.g., Kokott J and Sobotta C. The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR, *International Data Privacy Law* 2013, 3(4): 222–228, 222.
[13] See, e.g., Land KM and Aronson DJ (eds.). *New Technologies for Human Rights Law and Practice*. Cambridge University Press, 2018.
[14] See, e.g., Kinfe Y. *Privacy and the Role of International Law in the Digital Age*. Oxford University Press, 2023, 76.
[15] See, e.g., Gregorio De G and Radu R. Digital constitutionalism in the new era of Internet governance. *International Journal of Law and Information Technology* 2022, 30(1): 68–87, 68.

making it challenging to address and explain how Big Data analytics threatens the interests of people.

1.3. Purpose

The thesis aims to achieve several purposes: description, explanation, evaluation, and legal reform. Firstly, the thesis aims to systematically describe the scope of the right to privacy, its development, and its application. It also analyses its relationship with data protection and objectively assesses the overall functioning of the two legal regimes. Secondly, it aims to explain the causal relationship between the privacy threats posed by Big Data analytics and the shrinking boundaries of informational self-determination. Thirdly, the thesis critically evaluates the adequacy of evolutive interpretation in adapting the right to privacy under Article 17 of ICCPR to the digital age. Finally, based on research evaluations, the thesis outlines legal reform in international privacy law.

1.4. Objective and Research Question

The objective of the thesis is to critically examine the overlap between privacy and data protection and generate the necessary reform of international privacy law. In light of the purpose and objective of this thesis, the following research question will be addressed:

To what extent does the evolutive interpretation of the right to privacy ensure the standards of informational self-determination in the digital age? What alternative solution may be needed to strengthen the ability of individuals to enjoy informational self-determination?

The following sub-questions will be briefly analysed insofar as they provide elements useful to answer the main research question.

Sub-questions:

1. *What are the main benefits and shortcomings of evolutive interpretation of the right to privacy in the digital age?*

2. *In what specific ways does Big Data analytics hinder the individual's ability to exercise informational self-determination?*

3. *How can recognising the right to data protection improve informational self-determination in the digital age?*

4. *What is the most feasible way of implementing the right to data protection into existing international human rights law?*

1.5. Methodology and Materials

Apart from the systematic literature review presented in Section 1.2., this work uses several methods in the individual chapters.

The legal doctrinal method "provides a systematic exposition of the rules governing a particular legal category, analyses the relationship between rules, explains areas of difficulty and, perhaps, predicts future developments."[16] Accordingly, Chapters 2 and 3 utilise the legal doctrinal method to define the concepts and gaps of evolutive interpretation, the right to privacy, and informational self-determination. As the method makes "a unique blend, of deduction and induction, the conceptual analysis of law and creative synthesis together"[17] builds up the legal proposition for legal reform in Chapter 5.

The thesis also deploys a literature review. The basic task of the literature review is to contextualise the issues, unravel the domain of previous thoughts, and set up bridges between the research project and the current state of knowledge.[18] In Chapter 3, this method assists in identifying specific challenges of the use of Big Data processing tools and the ways these challenges undermine the tenets of informational self-determination.

The comparative method "enables us to draw inferences about similarities and differences"[19] between the right to privacy and data protection amidst the provisions of international law in Chapter 4 and "develop a substantive theory."[20]

[16] Ishwara PB. *Idea and Methods of Legal Research*. Oxford University Press, 2019, 11.
[17] Ibid., 145.
[18] Ibid., 116.
[19] Ibid., 29.
[20] Ibid.

The analytical method is a part of the legal doctrinal method. It analyses what the law is by relating the legal norm to the hierarchy of international norms, finding its meaning through the application of principles of statutory interpretation, and synthesising the overall principle in a coherent manner.[21] Since this work aims at proposing a legal reform of international privacy law, in Chapter 5, the analytical method is instrumental in determining the flaws of current legal regulation and presenting a new approach to privacy and data protection that addresses existing gaps in international law.

As regards the materials, international law makes up the core of the thesis. The 1946 Statute of the International Court of Justice, Article 38, identifies a list of sources of International Law.[22] Respectively, the thesis examines the following treaties: ICCPR, the 1969 Vienna Convention on the Law of Treaties[23] (VCLT); Jurisprudence by the International Court of Justice (ICJ) and the UN Human Rights Committee. Other material sources of international law include resolutions adopted by the UN General Assembly and the UN Human Rights Council, as well as a source of an authoritative interpretation of international law, namely, General Comment 16.

1.6. Delimitations

While the Charter of Fundamental Rights of the European Union[24] (CFREU) has acknowledged the right to data protection and the European Court of Human Rights (ECtHR) has expanded upon it through its case law,[25] the focus of this thesis revolves around the lack of recognition of data protection in Article 17 of the ICCPR. The CFREU is utilised to demonstrate the fragmentation of privacy regulations on both regional and international levels, and relevant cases from the ECtHR are cited as supporting evidence for the presented arguments.

---

[21] Ibid.

[22] UN, Statute of the International Court of Justice (1946) Treaty Series 993, Art. 38(1) identifies the following sources:
(a) Treaties between States;
(b) Customary international law derived from the practice of States;
(c) General principles of law recognised by civilised nations;
(d) Judicial decisions and the writings of the most highly qualified publicists.

[23] UN, Vienna Convention on the Law of Treaties (1969) Treaty Series 1155.

[24] EU, Charter of Fundamental Rights of the European Union (2012) 2012/C 326/02, Art. 8.

[25] See, e.g., European Court of Human Rights, *Amann v Switzerland* (2000) Application No. 27798/95, para 65; European Court of Human Rights, *Rotaru v Romania* [Grand Chamber] (2000) Application No. 28341/95., para 43.

In addition to privacy concerns, Big Data analytics raises many issues related to ethics and discrimination. While these issues are also important and deserve attention, in the scope of this research, the literature review indicated that privacy is more urgent since the digital environment was built and continues to develop with limited consideration of privacy.

Big Data analytics serves as a primary example in connection to contextual examples. Indeed, many emerging technologies raise privacy concerns. However, unlike other technologies, Big Data processing tools are defined by their size and complexity, with the potential to collect and process vast amounts of data from various sources. Thus, focusing on Big Data analytics allows for a more focused and in-depth analysis of the challenges presented by contemporary data-driven technologies.

Finally, the term "Big Data analytics" is broad and technical. Thereby, the focus is on collecting large amounts of data from an array of digital sources. Given the legal nature of the thesis, explanations of technical aspects and methods are limited.

1.7. Outline

This thesis contains six chapters, including the introductory chapter, in order to answer the research questions. By displaying the role of evolutive interpretation, Chapter 2 systematically describes the scope of the right to privacy and its normative gaps. It also concludes that one of the main issues in international privacy regulation is the need for a more precise division between the right to privacy and data protection. Chapter 3 "confronts" the right to privacy with practical challenges posed by Big Data analytics to examine the effects of identified gaps on informational self-determination. Chapter 4 establishes distinctions between privacy and data protection and contextualises the interplay between the two regimes. Respectively, Chapter 5 sets forth a new approach to repair fragmentation in international privacy regulation and ensure the tenets of informational self-determination: the right to data protection as a separate human right next to privacy. Finally, Chapter 6 summarises key findings and presents conclusions.

2. EVOLUTIVE INTERPRETATION OF THE RIGHT TO PRIVACY IN THE INTERNATIONAL LEGAL FRAMEWORK

2.1. Concept of Evolutive Interpretation

Treaties can evolve as a result of evolutive interpretation. Article 31(1) of the VCLT provides that a treaty shall be interpreted "in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose."[26] The 2009 case of Navigational Rights of the ICJ explains the meaning of evolutive interpretation in practice. The question under review was whether the phrase "for the purposes of commerce" in the 1858 treaty of limits between Nicaragua and Costa Rica covered tourism, i.e., the carriage of passengers for hire. The ICJ held that the phrase must be interpreted so as to cover all modern forms of commerce, including tourism.[27] "'Where the parties have used generic terms in a treaty, the parties necessarily had to have been aware that the meaning of the terms was likely to evolve over time, and where the treaty has been entered into force for a very long period,' the Court said, 'the parties must be presumed, as a general rule, to have intended those terms to have an evolving meaning.'"[28]

Human rights courts also apply evolutive interpretation in their jurisprudence. For example, "the ECtHR has taken a broad, evolutive view on Article 8 the Right to Privacy" [29] of the 1950 European Convention on Human Rights (ECHR).[30] In Tyrer v. United Kingdom, the ECtHR held that the ECHR is "a living instrument to be interpreted in the light of present-day conditions."[31] The Inter-American Court of Human Rights has taken this approach in several cases: "human rights treaties are live instruments whose interpretation must adapt to the evolution of the times and, specifically, to current living

[26] UN, Vienna Convention on the Law of Treaties (1969) Treaty Series 1155, art. 31(1).
[27] International Court of Justice, *Dispute regarding Navigational and Related Rights (Costa Rica v Nicaragua)* (2009) Judgement I.C.J. Reports, p. 213, para 71.
[28] Ibid., para 66.
[29] Bygrave LA. Data Protection Pursuant to the Right to Privacy in Human Rights Treaties. *International Journal of Law and Information Technology* 1998, 6(3): 247–284, 253.
[30] Council of Europe, European Convention on the Protection on Human Rights and Fundamental Freedoms (1950) Treaty Series 5.
[31] European Court of Human Rights, *Tyrer v United-Kingdom* (1978) Application No. 5856/72, para 31.

conditions."[32] The African Commission on Human and Peoples' Rights has also adopted a living instrument approach in interpreting the term "peoples" to extend it to indigenous groups.[33]

The UN human rights treaty bodies have implemented a similar approach to general international law and regional human rights courts. In Judge v. Canada, the UN Human Rights Committee said regarding the ICCPR that it "should be interpreted as a living instrument and the rights protected under it should be applied in context and in the light of present-day conditions."[34] The phrase "living instrument" has become a reference to a rapidly changing situation in human rights law at the international, regional, and national levels.

Evolutive interpretation is considered especially well suited for interpreting human rights treaties. Rudolf Bernhardt, a former President of the ECtHR, argued that evolutionary interpretation is particular to human rights treaties. According to R. Bernhardt, "although the provisions on treaty interpretation contained in the VCLT on their face seem to make no distinction between different types of treaties, this ought not to detract from the fact that the object and purpose of human rights treaties set them apart from other types of a treaty."[35] "The impression that the principles of treaty interpretation apply similarly to all types of treaty, he says, is either misleading or else correct only on a highly abstract level; when it comes to human rights treaties, he concluded, the traditional rules of treaty interpretation need some adjustment."[36]

The discussions on whether the right to privacy in international human rights law fits the digital age draw even more attention to the evolutive interpretation. In stating that international human rights law provides the universal privacy framework, the former UN High Commissioner for Human Rights Navanethem Pillay implied that there are no blind

[32] See, e.g., Inter-American Court of Human Rights, *The Mayagna (Sumo) Awas Tingni Community v Nicaragua* (2008) Judgement 136 International Law Reports 73, paras 146-148; Inter-American Court of Human Rights, *Bámaca-Velásquez v Guatemala* (2000) Judgement C Series No. 70, para 158; Inter-American Court of Human Rights, *the Gómez-Paquiyauri Brothers v Peru* (2004) Judgement C Series No. 110, para 165.

[33] African Commission on Human and People's Rights. *Centre for Minority Rights Development (Kenya) and Minority Rights Group International on Behalf of Endorois Welfare Council v Kenya* (2010) Communication 276/2003, paras 151, 154, 157.

[34] UN Human Rights Committee, *Roger Judge v Canada* (2003) CCPR/C/78/D/829/1998, para 10.3.

[35] Bjorge E. *The Evolutionary Interpretation of Treaties*. Oxford University Press, 2014, 12.

[36] Ibid.

spots in the current privacy framework.[37] Moreover, Professor Anja Seibert-Fohr, a former member of the UN Human Rights Committee and the current judge of the ECtHR, argues that there is no "blind spot" in the international law of privacy and what is lacking is national-level regulation.[38] The Professor suggests that the Human Rights Committee's "evolutive interpretation" has allowed it to "confront new challenges and keep human rights protection alive and effective based on the existing legal framework."[39]

The outlined jurisprudence by the ICJ, regional human rights courts, and the UN Human Rights Committee, together with academic publications by judges and UN officers, directly and indirectly, demonstrates that evolutive interpretation plays a role in developing human rights, including the right to privacy. Thus, the following sections systematically describe the scope and normative gaps of the right to privacy and examine whether and to what extent evolutive interpretation is a sufficient tool to uphold the right in the digital age.

2.2. International Human Rights Law Framework of the Right to Privacy

Against the above backdrop, this section describes the right to privacy according to the ICCPR, the UN Human Rights Committee jurisprudence, the UN soft law instruments, and General Comment 16. Gradually, source by source, this section will map out the scope of the right to privacy and its normative gaps. As shall become apparent, the evolution of the right to privacy has resulted in two overlapping regimes: privacy and data protection.

2.2.1. International Covenant on Civil and Political Rights

At the core of international human rights instruments lies the ICCPR. The ICCPR is the principal treaty of universal scope that guarantees the right to privacy. Article 17 of ICCPR states:

[37] Kinfe Y. *Privacy and the Role of International Law in the Digital Age*. Oxford University Press, 2023, 76.
[38] Ibid., 77.
[39] Ibid.

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks.[40]

The right to privacy protects an area of autonomous development and liberty, a "private sphere" that shall not be infringed by the unsolicited interventions of state actors, individuals, or corporations.[41] However, the right to privacy has not received as much attention during the drafting as other rights that found relatively clear formulations in the Covenant.[42] It means "that not only the drafting exercise was plagued by urgency but also that themes that received significant discussion during the drafting did not include the right to privacy."[43] The result of it is a lasting impact and several issues related to the scope of the right to privacy.

Firstly, the scope of the right is vague. The right to privacy protects different values: privacy, home, family, and correspondence. The jurisprudence of the UN Human Rights Committee extends this circle of values even further. For instance, the Committee had found that the right to privacy was violated when people were not allowed to change their names for religious purposes,[44] when a general prohibition of homosexuality was introduced,[45] and when a state deprived the ancestral burial territory of members of an indigenous population.[46] The expansive understanding of the right to privacy illustrates the challenges of defining its boundaries, encompassing not only traditional aspects such as privacy, home, family, and correspondence but also extending to diverse areas like religious freedoms, sexual orientation, and indigenous rights. The broadened

[40] UN General Assembly, International Covenant on Civil and Political Rights (1966) Treaty Series 999, Art. 17.
[41] Bignami F and Resta G. Human Rights Extraterritoriality: The Right to Privacy and National Security Surveillance. Benvenisti E and Nolte G (eds). *Community Interests Across International Law*. Oxford University Press, 2018, 3.
[42] Kinfe Y. *Privacy and the Role of International Law in the Digital Age*. Oxford, 2023, 37.
[43] Ibid., 34.
[44] UN Human Rights Committee, *Coeriel and Aurik v Netherlands* (1994) Communication No. 453/1991, U.N. Doc. CCPR/C/48/D/453/1991, para 10.2.
[45] UN Human Rights Committee, *Toonen v Australia* (1994) Communication No. 488/1992, U.N. Doc. CCPR/C/50/D/488/1992., para 8.6.
[46] UN Human Rights Committee, *Francis Hopu and Tepoaitu Bessert v France* (1997) Communication No. 549/1993, U.N. Doc. CCPR/C/60/D/549/1993/Rev.1., para 10.3.

interpretation highlights the need for greater clarity to ensure a balanced and coherent application of privacy rights in a rapidly evolving societal landscape.

Secondly, unlike other covenant rights, such as freedom of expression, the provision lacks a limitation clause aside from the generic qualifying terms "arbitrary" and "unlawful". The provision is framed essentially in terms of a prohibition on interference with privacy. The UN Human Rights Committee has filled the legal vacuum by interpreting these terms in General Comment 16[47] to reflect the three-part test of legality, necessity, and legitimacy. While this interpretation helps to fill the gap, the reliance on a non-binding document raises concerns about the consistency and enforceability of privacy rights across different jurisdictions.

Thirdly, Article 17 of the ICCPR falls short of explicitly stipulating data protection guarantees, a vital framework for safeguarding the right to privacy in the digital age. As the following chapters will demonstrate, the absence of specific references to data protection within the ICCPR poses a significant concern. However, there are indications of efforts being made to address this gap. In General Comment 16, the UN Human Rights Committee has emphasised the necessity of legally implementing essential data protection guarantees across both the public and private sectors in accordance with Article 17.[48] Furthermore, the reference in Article 17(2) to the "right to the protection of the law" can be construed in conjunction with Article 2(2) of the ICCPR, which defines the general duty of State parties to adopt legislation or other measures as may be necessary to give effect to the rights recognised in the Covenant.[49] It is evident that the ICCPR alone neither explicitly mentions data protection nor adequately captures its intricate relationship with privacy.

In summary, flaws of Article 17 emerge from its vague scope and poor formulation. The concept of privacy has evolved to encompass a wide range of normative values, interests, and areas of protection that surpass the original confines of Article 17. This expansion, on the one hand, reflects the progression of the article. On the other hand, it contributes to the lack of clarity and misuse of various terms and definitions associated

[47] UN Human Rights Committee, *CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, 1988, para 8.
[48] Ibid., para 10.
[49] Kinfe Y. *Privacy and the Role of International Law in the Digital Age*. Oxford University Press, 2023, 39.

with privacy, as they are often mistakenly used interchangeably. Crucially, while authoritative interpretations surrounding Article 17 shed light on the fundamental principles of data protection inherent in the right to privacy, the provision lacks clarity regarding the explicit role of data protection within the broader privacy framework. This ambiguity hampers the establishment of a coherent and comprehensive legal foundation for safeguarding privacy rights in an increasingly data-centric world.

2.2.2. UN Human Rights Committee Jurisprudence

The preceding section has brought to light the lack of diligence and precision in the evolution of the right to privacy. The abbreviated form of the right necessitates a closer examination of jurisprudence to verify whether it adequately addresses the deficiencies of Article 17. In this regard, the UN Human Rights Committee takes centre stage by primarily deliberating on cases of the right to privacy under the ICCPR.

In its case law, namely, in the Coeriel and Aurik v. the Netherlands, the Committee has defined the notion of privacy in Article 17 as not only a sphere of seclusion for oneself; but also "a sphere of a person's life in which he or she can freely express his or her identity, be it by entering into relationships with others or alone."[50] It reveals that the UN Human Rights Committee has given a considerable potential for the expansion of the notion of privacy. Accordingly, this decision indicates that the notion of "private life" "should not be interpreted narrowly; in other words, to be protected under Article 17, data on a person's private life need not refer only to what the person does in the intimacy of his/her home but also to, say, his/her professional activities."[51] It proves that there is no reason for limiting the application of Article 17 to situations in which personal data is collected, stored, or further processed by computerised or automated methods.

Only a limited number of cases tackle contemporary privacy issues caused by technologies. Most privacy cases adjudged by the UN Human Rights Committee concern the right to family life of foreigners facing expulsion orders, the right not to be subjected to unreasonable search and seizure or interference with the secrecy of prisoners'

[50] UN Human Rights Committee, *Coeriel and Aurik v the Netherlands* (1994) Communication No. 453/1991, U.N. Doc. CCPR/C/48/D/453/1991, para 10.2.
[51] Bygrave LA. Data Protection Pursuant to the Right to Privacy in Human Rights Treaties. *International Journal of Law and Information Technology* 1998, 6(3): 247–284, 253.

correspondence.[52] The analysis of the Human Rights Committee's case list reveals only four privacy cases involving digital communications such as the internet and telecommunications, as well as the disclosure of personal information.[53]

However, these cases only scratch the surface when addressing the complexities of digital privacy. For example, in Nabil Sayadi and Patricia Vinck v. Belgium, the Committee evaluated the issue in terms of reputation and honour rather than privacy. It deemed the publication of full contact details of the authors through their inclusion on the Sanctions Committee's list as an attack on their honour and reputation.[54] In the case of Antonius Cornelis Van Hulst v. Netherlands, the Committee resolved the case by applying the test according to which an interference with the right to privacy is permissible under Article 17 if "it is provided by law, is in accordance with the provisions, aims and objectives of the Covenant and is reasonable in the particular circumstances of the case."[55] Finally, in IP v. Finland and HS v. Australia, the Committee has hardly even addressed the cases in their entirety as it found the claims were not substantiated.[56] Therefore, the decisions are not backed by a thorough examination.

In summary, the jurisprudence of the Human Rights Committee utilised evolutive interpretation to address some of the deficiencies of Article 17. For example, it clarified the notion of privacy and significantly expanded its scope. In addition, it implied that Article 17 applies to cases concerning data protection. However, the issues of a truncated formulation of Article 17 and an inadequate elaboration of the relationship between privacy and data protection remain. Thus, the Human Rights Committee's jurisprudence seems to contribute to the fragmentation of the international privacy framework by increasing the overlap between various interests and focusing on competing values such

[52] See, e.g., UN Human Rights Committee, *Khaoukha Marouf v Algeria* (2014) Communication No 1889/ 2009, U.N. Doc. CCPR/C/110/D/1889/2009.
[53] See, e.g., UN Human Rights Committee, *I. P. v Finland* (1993) Communication No. 450/1991, U.N. Doc. CCPR/C/48/D/450/1991; UN Human Rights Committee, *Antonius Cornelis Van Hulst v the Netherlands* (2004) Communication No. 903/1999, U.N. Doc. CCPR/C/82/D/903/1999; UN Human Rights Committee, *Nabil Sayadi and Patricia Vinck v Belgium* (2008) Communication No. 1472/ 2006, U.N. Doc. CCPR/C/94/D/1472/2006; UN Human Rights Committee, *H.S. v Australia* (2015) Communication No. 2015/2010, U.N. Doc. CCPR/C/113/D/2015/2010.
[54] UN Human Rights Committee, *Nabil Sayadi and Patricia Vinck v Belgium* (2008) Communication No. 1472/ 2006, U.N. Doc. CCPR/C/94/D/1472/2006, para 10.2.
[55] UN Human Rights Committee, *Antonius Cornelis Van Hulst v Netherlands* (2004) Communication No. 903/1999, para 7.3.
[56] See, e.g., UN Human Rights Committee, *I. P. v Finland* (1993) Communication No. 450/1991, para 6.3; UN Human Rights Committee, *H.S. v Australia* (2015) Communication No. 2015/2010, U.N. Doc. CCPR/C/113/D/2015/2010, para 8.12.

as reputation and honour rather than taking an opportunity to provide a thorough legal analysis of privacy.

2.2.3. UN Soft Law Instruments

Soft law has contributed to the development of the right to privacy in international human rights law. The Universal Declaration of Human Rights, a soft law document adopted through a resolution of the UN General Assembly, first recognised the right to privacy. Not only has it been translated into hard law with the adoption of the ICCPR, but most of its rights have arguably become rules of general international law. To this day, soft law plays a crucial role in the evolution of the right to privacy, partly due to the evolutive interpretation. To enhance clarity, Figure 1 is a visual metaphor of the prevalence of evolutive interpretation in the UN soft law instruments.

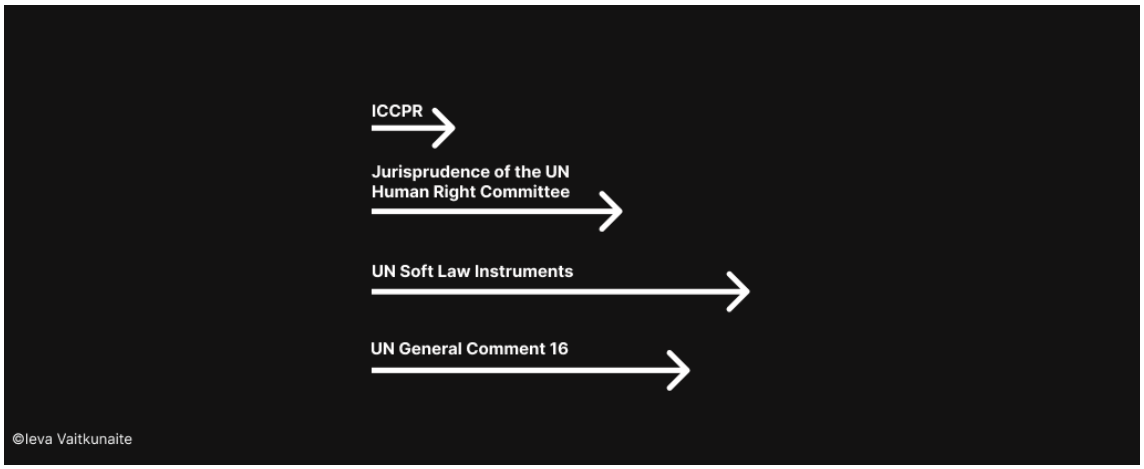

Figure 1 *An abstract visualisation of the prevalence of evolutive interpretation across examined sources of international law*

Evolutive interpretation in soft law exists in reimagining and revitalising the right to privacy to make it fit for purpose in the digital age. Through the post-Snowden[57] privacy discourse, soft law is making an important contribution to elaborating questions

[57] Edward Snowden, a former National Security Agency contractor, leaked classified information in 2013 that exposed the extent of global surveillance programs conducted by the United States and its allies. Snowden's revelations revealed that the NSA collected vast amounts of phone and internet data on foreign and US citizens. It included the bulk collection of phone metadata and the interception of emails, social media communications, and other internet traffic. The disclosures sparked a global debate on the balance between privacy and security, with many arguing that the programs violated individual privacy rights and lacked sufficient oversight and transparency.

related to privacy. The discourse introduced progressive standards on the right to privacy by virtue of a series of resolutions adopted by both the UN General Assembly and the UN Human Rights Council. The resolutions incorporate principles of privacy and governance norms that had no prior recognition in public international law. The following selection highlights the evolutionary impact of these standards on the international privacy framework:

1) Data protection regulation. The UN General Assembly Resolution 73/179 calls upon all States "[t]o consider adopting and implementing data protection legislation, regulation and policies, including on digital communication data, that comply with their international human rights obligations, which could include the establishment of independent national authorities with powers and resources to monitor data privacy practices, investigate violations and abuses and receive communications from individuals and organizations, and to provide appropriate remedies."[58] This clause is the most explicit call for States to enact and implement data protection legislation that regulates the processing of personal data and installs national supervisory bodies.
2) Corporate responsibility. The UN General Assembly Resolution 75/176 calls upon technology companies to implement data subject rights to personal access data, to rectification of inaccurate data, and erasure of personal data.[59] The resolutions envisage notions of privacy impact assessment, data protection by design and data breach notification.[60] As part of the call on technology companies to implement administrative, technical, and physical safeguards, a series of data protection principles are recognised, namely principles of purpose limitation, data minimization, data quality, data security, and lawful processing.[61]
3) Emerging technologies. The UN General Assembly Resolution 73/179 not only recognises novel threats posed by the rapid growth of automated technologies like Artificial Intelligence and machine learning but also emphasises the need to align

[58] UN General Assembly Resolution, *The right to privacy in the digital age,* A/RES/73/179, 2018, para 6(g).
[59] UN General Assembly Resolution, *The right to privacy in the digital age*, A/RES/75/176, 2020, para 8(e).
[60] Ibid., paras 8(c)-(d), (f).
[61] Ibid., para 8(c).

their "design, evaluation and regulation" with international human rights law.[62] The Human Rights Council Resolution 48/4, for instance, also calls upon States to protect individuals from harm caused using automated processes.[63]

In summary, as depicted in Figure 1, evolutive interpretation has significantly influenced soft law instruments. As previously illustrated, these resolutions have introduced principles of data protection regulation that were previously absent from international law, thereby shaping the normative boundaries of the right to privacy. Additionally, they not only address emerging technological challenges and the role of corporate responsibility, but also affirm the trend of integrating data protection within the privacy framework, which has been lacking in jurisprudence for a considerable period. Despite this confirmation, numerous questions remain regarding the interaction between the right to privacy and data protection.

2.2.4. General Comment 16

Although General Comments of the Human Rights Committee receive varied reception by States, international, and national courts, they "are central to understanding human rights treaty obligations and have been described as 'indispensable' sources of interpretation."[64] "General Comments are 'secondary soft law instruments', meaning sources of non-binding norms that interpret and add detail to the rights and obligations contained in the respective human rights treaties."[65] Hence, "the oft-heard phrase is that General Comments contain 'authoritative' statements or interpretations of the Covenant."[66] The right to privacy has a designated General Comment 16, which the UN Human Rights Committee drafted during its early phases of work in 1988. While useful in its insights about the core concepts in Article 17, the document is just over two pages long.

[62] UN General Assembly Resolution, *The right to privacy in the digital age,* A/RES/73/179, 2018, preamble para 19, para 7(d).
[63] UN Human Rights Council Resolution, The *right to privacy in the digital age,* A/HRC/RES/48/4, 2021.
[64] Keller H and Grover L. General Comments of the Human Rights Committee and their legitimacy. In Keller H and Ulfstein G (eds.), *UN Human Rights Treaty Bodies: Law and Legitimacy*. Cambridge: Cambridge University Press, 2012, 118.
[65] Ibid., 129.
[66] UN Human Rights Committee, *CCPR General Comment No. 33: Obligations of States parties under the Optional Protocol to the International Covenant on Civil and Political Rights*, 2008, para 13.

To begin with, the General Comment reference some technologies and modes of communication. However, in light of the current state of global surveillance infrastructure, these references may seem rather outdated. The Comment acknowledges that:

> "[s]urveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited."[67]

The above paragraph illustrates that General Comment 16 is grounded in a context where the internet was still in its early stages — long before the possibility of instant communication through electronic mail, instant messaging and the proliferation of discussion forums, blogs, social networks, and online shopping platforms. Consequently, it is unsurprising that the General Comment fails to provide specific guidance on how privacy should be comprehended in a world dominated by technology.

Another critical passage references the collection, storage, and use of personal data on electronic databases:

> "The gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law. Effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process and use it, and is never used for purposes incompatible with the Covenant."[68]

As outlined in Section 2.2.1., this paragraph requires the legal implementation of essential data protection guarantees in both the public and private sectors. It signifies that the right to privacy encompasses crucial principles to safeguard personal data.

However, the General Comment has no reference to the internet or even newer communication technologies and no examination of their impact on privacy interests. There is no anticipation of the evolution from fixed-line telephone systems to mobile telecommunications on a large scale; the emergence of Big Data analytics; the

[67] UN Human Rights Committee, *CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation,* 1988., para 8.
[68] Ibid., para 10.

relationships between Big Tech companies and governments; or the ability to track internet activities on a large scale through social media monitoring.

To conclude, General Comment 16 asserts that the right to privacy should be protected de jure and de facto, and surveillance is prohibited under Article 17. It also offers some insights into the interplay between the ICCPR's guarantee of the right to privacy and domestic data protection laws. However, it is essential to note that General Comment 16 relies on an outdated understanding of communications infrastructure, leaving space for further elaboration on data protection, which Chapter 5 will explore.

2.3. Main Benefits and Shortcomings of Evolutive Interpretation

The digital age has introduced novel human rights challenges requiring a progressive legal interpretation to adapt laws to the new realities. In this regard, evolutive interpretation is instrumental in elaborating on legal provisions in light of the contemporary landscape. It holds particular significance in discussions concerning the applicability of the right to privacy, considering that this right was initially formulated in an era predating the internet and the technological revolution. Evolutive interpretation, therefore, re-evaluates the right to privacy to ensure its vitality and enduring relevance.

Evolutive interpretation offers various benefits for human rights. It enables a more expedited and streamlined evolution of legal provisions, ensures adaptability to changing circumstances, and contributes to the ongoing advancement of international human rights law. However, these benefits are accompanied by certain shortcomings. The jurisprudence of the UN Human Rights Committee has moved towards a recognition of various data protection guarantees on a case-by-case basis. "These guarantees have tended to be linked to the concrete circumstances of the particular case, making it difficult to apply them more generally."[69]

It is crucial to highlight that the development of law should prioritise rationality and precision to ensure stability and clarity. In this regard, evolutive interpretation has limitations in meeting these objectives. Adapting legal norms to novel circumstances often results in a more reactive rather than proactive regulatory approach. While evolutive

[69] Bygrave LA. Data Protection Pursuant to the Right to Privacy in Human Rights Treaties. *International Journal of Law and Information Technology* 1998, 6(3): 247–284, 253.

interpretation serves as a valuable tool to redefine certain aspects of privacy in response to emerging technological threats, it is insufficient for addressing more intricate issues. For instance, navigating the fragmentation between privacy and data protection at the international level requires additional guidance.

Furthermore, the inherent flexibility of evolutive interpretation can inadvertently lead to a regression in privacy laws. It is essential to acknowledge that the UN human rights treaty bodies are not immune to subjectivity or institutional biases in some issues. Less democratic States, holding influence within these institutional bodies, may exploit evolutive interpretation to restrict the right to privacy. Thus, evolutive interpretation runs the risk of undermining the strength of human rights and being exploited to restrict the right to privacy instead of fostering its advancement.

Apart from technical deficiencies and politically motivated restrictions, evolutive interpretation perpetuates the misconception that the right to privacy, as originally drafted in 1954, is fully adaptable to the digital age. This approach is detrimental as it prevents the much-needed comprehensive reform of the international privacy framework, essential for addressing fundamental shortcomings within the scope of the right to privacy.

Upon thorough analysis, it becomes evident that Article 17 of the ICCPR[70] exhibits several shortcomings. These include its vague scope, poor formulation, linguistic inconsistencies, and the tendency to confuse privacy with a multitude of other values, interests, and zones of protection. Relying on legal provisions riddled with gaps to construct a new privacy framework is detrimental, particularly within international human rights law, which aims to establish universal standards.

Drawing from this analysis, it becomes apparent that evolutive interpretation has limitations in adapting the normative right to the demands of the digital age. Urgent reforms to the privacy framework are necessary, given the continuous deployment of new technologies in an unregulated landscape. While it can be concluded that evolutive interpretation contributes to the advancement of international privacy regulations, it is not equipped to address substantial gaps within the existing privacy framework.

In conclusion of this chapter, the notion that the current legal framework of privacy is well developed or that evolutive interpretation can fill every legal disparity

[70] UN General Assembly, International Covenant on Civil and Political Rights (1966) Treaty Series 999, Art. 17.

caused by technological changes is misguided. This chapter has demonstrated that the right to privacy is not only plagued with normative gaps but also that the evolution of the right has created two conflated legal frameworks within international human rights law: privacy and data protection. Therefore, the right to privacy must take a different direction in its development to accommodate informational self-determination – a significant concept in digital privacy. Thus, the subsequent chapter delves into the implications of the challenges of Big Data analytics on informational self-determination when they intersect with the right to privacy.

3. INFORMATIONAL SELF-DETERMINATION AND BIG DATA ANALYTICS

3.1. Concept of Informational Self-Determination

While Chapter 2 laid out the conventional scope of the right to privacy, this chapter demonstrates the complexity of privacy challenges in practice. This chapter begins with the definition of information self-determination. It discusses three mutually reinforcing challenges that Big Data processing tools exhibit and subsequently undermine informational self-determination: transnationalism of privacy threats, little-regulated private actors, and sophistication of privacy threats.

The concept of informational self-determination originates from the landmark Census decision of the German Constitutional Court.[71] According to the Constitutional Court, the right to informational self-determination guarantees, in principle, the power of the individual to determine for himself the disclosure and use of his or her data. This right is based on Article 1(1) *human dignity*[72] and Article 2(1) *personality right*[73] of the German Constitution. These provisions require "'clearly defined conditions of processing,' which ensure 'that under the conditions of automatic collection and processing of personal data, the individual is not reduced to a mere object of information.'"[74] The main aspects of informational self-determination are context and control over the flow of personal information. This ties in with the concept of purpose limitation,[75] which is among the core privacy requirements.[76]

Similarly, the ECtHR has also acknowledged that individual self-determination is an important principle underlying privacy. Though no previous case has established the right to self-determination as contained in Article 8 "the Right to Respect for Private and

[71] German Federal Constitutional Court, *Order of the First Senate* (1983) 1 BvR 209/83, paras 1-214.
[72] German Bundestag, Basic Law for the Federal Republic of Germany (1949) in the revised version published in the Federal Law Gazette Part III, classification number 100-1, as last amended by the Act of 28 June 2022, Art. 1(1).
[73] Ibid., Art. 2(1).
[74] Tzanou M. Data Protection as a Fundamental Right Next to Privacy? 'Reconstructing' a not so New Right, *International Data Privacy Law* 2013, 3(2): 88–99, 89.
[75] According to Lee Bygrave, personal data should be gathered for specified and lawful purposes and not processed in ways that are incompatible with those purposes. Bygrave LA. Data Protection Pursuant to the Right to Privacy in Human Rights Treaties. *International Journal of Law and Information Technology* 1998, 6(3): 247–284, 250.
[76] Strauß S and Nentwich M. Social Network Sites, Privacy and the Blurring Boundary Between Public and Private Spaces, *Science and Public Policy* 2013, 40(6): 724–732, 727.

Family Life" of the ECHR,[77] the Court considered that the notion of personal autonomy is an important principle underlying the interpretation of its guarantees. In Pretty v. the United Kingdom, the ECtHR asserted that "private life" is a broad term encompassing, inter alia, aspects of an individual's physical and social identity, including the right to personal autonomy, personal development, and to establish and develop relationships with other human beings and the outside world.[78]

The concept of informational self-determination derives from the right to privacy but not the classical meaning of "privacy" or "secrecy". Instead, it refers to another dimension of privacy, i.e., individual autonomy, the capacity to make choices, to make informed decisions, in other words, to keep control over certain aspects of one's life.[79] The notion of "control" in this context not only implies the capacity to decide over the use of one's data but also encompasses the right to be aware of the fate of that data, to get informed about who knows what about you and what to do.[80]

The technical means of storing information, the automatic data processing, and combining data in integrated information systems add up to a partial or virtually complete personality profile. However, individuals often lack adequate means to control the accuracy and usage of such profiles effectively. Therefore, the right to informational self-determination becomes increasingly crucial in the digital age. It precludes a social order in which citizens can no longer know who knows what, when, and on what occasion about them.[81] As such, the lack of it would "[n]ot only impair opportunities of personal development for the individual, it would also affect the common good because self-determination [is] a fundamental prerequisite for the functioning of a free and democratic society which relies on the agency and participation of its citizens."[82]

[77] Council of Europe, European Convention on the Protection on Human Rights and Fundamental Freedoms (1950) Treaty Series 5, Art. 8.
[78] European Court of Human Rights, *Pretty v The United Kingdom* (2002) Application No. 2346/02, para 61.
[79] De Terwangne C. The Right to be Forgotten and Informational Autonomy in the Digital Environment. Ghezzi A et al. (eds). *The Ethics of Memory in a Digital Age*. Palgrave Macmillan Memory Studies. Palgrave Macmillan, London, 2014, 4.
[80] Ibid.
[81] German Federal Constitutional Court, *Order of the First Senate* (1983) 1 BvR 209/83, paras 1-214, para 146.
[82] Ibid.

3.2. Challenges of Big Data Analytics to Informational Self-Determination

Big Data analytics is a catchphrase for various interrelated sociotechnical techniques, tools, and practices. "Big data analytics involves deploying a number of techniques and tools designed to find patterns, behavioural indicators, or identities of individuals, groups, or populations. Structuring data, performing statistical modeling, and creating visualisations transform otherwise incomprehensible datasets into actionable information."[83] The analysis relies on the collection of large amounts of data from an array of digital sources and sensors. The collection often occurs unbeknownst to those who are data subjects. In Big Data, the subjects create content or emit information about their everyday lives. For example, posting pictures on social media, navigating websites, or using a smartphone with GPS tracking operating in the background. Such data can be collected, processed, analysed, and visualised in order to glean social insights and patterns. Observation, decision-making, and direct action can utilise behavioural indicators at both the aggregate and individual levels.

The technology industry has made lucrative use of Big Data analytics to assess markets, predict consumer behaviour, identify trends, and train machine-learning algorithms. New information and communication technologies undoubtedly bring advantages and disadvantages across various domains. And so, when it comes to the human rights context, it is crucial to consider the potential risks associated with applying Big Data analytics.

One of the primary challenges arises from the digital landscape, which presents new possibilities for cross-border violation of the right to privacy. The global nature of Big Data technologies enables State and non-State actors to infringe upon individuals' privacy rights in multiple jurisdictions. While cross-border human rights violations are not unprecedented, the breadth of transnational privacy violations has grown exponentially with the global internet. The prevailing business model in cyberspace also entails the systematic corporate collection, processing, aggregation, and repurposing of personal data on a transnational scale. In the digital context, personal privacy can often be invaded by actors in jurisdictions well beyond the remit of data subjects' national legal

[83] Land KM and Aronson DJ (eds.). *New Technologies for Human Rights Law and Practice*. Cambridge University Press, 2018, 153.

systems. With the borderless nature of digital networks, these international actors can reach billions of users worldwide without any physical presence in the jurisdiction in question. This phenomenon can also be called the transnationalisation of privacy threats in the digital age.[84]

The second challenge stems from the proliferation of under-regulated private actors within the digital space. Private corporations now own and serve much of the internet's core physical and technical infrastructure as well as services.[85] Internet users worldwide heavily rely on these infrastructures and services, but most of these corporations operate under the jurisdiction of one or more specific States, which may themselves adopt diverging approaches to regulation. Furthermore, many goods and services offered in the internet space are governed through private contractual mechanisms between internet corporations and individual users. Often, these terms of use are unilaterally imposed and changed (and hence non-negotiable) and incomprehensible to lay users. "This state of affairs is increasingly transforming technology companies into 'competing centres of power', seemingly on par with governments when it comes to their ability to impact the enjoyment of human rights."[86] "With unprecedented access to and use of the personal data of billions of users worldwide, technology companies wield considerable influence"[87] over boundaries of informational self-determination.

The sophistication of privacy threats represents another challenge undermining informational self-determination. With the increasing adoption of Big Data analytics technologies, both governmental entities and corporations are strengthening their invasive practices. The ways in which the right to privacy could be undermined are becoming more seamless, surreptitious, and accessible. Not only are these technologies accessible by anyone with the economic means, but they can be, and are indeed, deployed to invade privacy across borders. As a result, privacy violations are facilitated, avenues for seeking remedies become more complex, and previously invasive practices tend to be normalised. The dynamic nature of the digital environment undercuts the effectiveness of orthodox protection mechanisms such as time-taking adjudicative processes.

[84] Kinfe Y. *Privacy and the Role of International Law in the Digital Age*. Oxford University Press, 2023, 2.
[85] Ibid.
[86] Ibid.
[87] Ibid.

To summarise, Big Data analytics comprises multiple challenges to privacy, including the potential for cross-border violations, the lack of adequate regulation for private actors, and the increasing sophistication of privacy risks. These challenges collectively indicate that the digital ecosystem has been developed without prioritising privacy concerns. Big Data analytics even perpetuates privacy risks and transgresses privacy norms. It, thus, leads to the next question of how these challenges impact the boundaries of informational self-determination.

3.3. Implications of Big Data Analytics on Informational Self-Determination

As discussed, the scope of informational self-determination refers to the right to control and manage personal data. It includes the right to know what data is collected, the right to object to the collection, processing, or sharing of data, the right to access and rectify personal data, and the right to data portability. Essentially, informational self-determination enables individuals to exercise control over how their personal information is used and shared, giving them autonomy and making informed choices about their privacy. Based on the challenges of Big Data analytics outlined in Section 3.2., this section examines how they limit the boundaries of informational self-determination.

3.3.1. Blurring the Line Between Personal vs. Public Spheres

First and foremost, the expansion of Big Data analytics blurs the boundaries between public and private spheres. The scope of informational self-determination covers not only sensitive data such as health and financial information but also information that may be less immediately sensitive that could still be used to identify or profile an individual, such as their browsing history or social media activity. Personal information and public user content can hardly be distinguished in these new environments.

In addition, the boundaries between personal and non-personal data become less distinct because the wide range of non-personal data can be used to reveal an individual's

identity, leading to the problem of the "identity shadow".[88] The term "identity shadow" refers to the digital trail of data that individuals leave behind when they engage in online activities. This data can include seemingly non-personal information, such as browsing history, search queries, and location data. However, it can unveil personal data when processed, posing potential privacy violations. In the process, one's informational self-determination and control over personal information are increasingly undermined. User information, preferences, behaviour, activities, or social relationships become explicitly visible.

The use of Big Data analytics challenges the distinction between sensitive and less sensitive information. A conflict arises between the users' intentions to share information and the ways Big Data processing tools use this information, for example, for behavioural targeting and processing of user data for commercial interests.[89]

3.3.2. Aggregation of Personal Data

Another way Big Data analytics impacts informational self-determination is by greatly exacerbating the dignitary harms associated with amassing information about a person—what Professor Daniel Solove calls aggregation.[90] With its massive scale, continuous monitoring from multiple sources, and sophisticated analytic capabilities, Big Data processing tools make aggregation more granular, revealing, and invasive. Of course, re-identification only heightens the harms associated with aggregation by enabling data controllers to link even more information to an individual's profile, leading to what is called the "database of ruin"[91].[92] The capability of Big Data analytics to map social

[88] Strauß S and Nentwich M. Social Network Sites, Privacy and the Blurring Boundary Between Public and Private Spaces, *Science and Public Policy* 2013, 40(6): 724–732, 727.
[89] Ibid.
[90] Rubinstein SI. Big Data: The End of Privacy or a New Beginning? *International Data Privacy Law* 2013, 3(2): 74–87, 77.
[91] According to Paul Ohm, the term "database of ruin" refers to the potential privacy risks that can arise from the accumulation and aggregation of vast amounts of personal data. It describes a hypothetical scenario in which a comprehensive database containing all conceivable information about an individual, including embarrassing or damaging details, is compiled. The concept highlights the concern that the increasing collection of personal data could lead to unintended consequences, such as the misuse or exposure of sensitive information. See, Ohm P. Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, *UCLA Law Review* 2010, 57: 1701–1777, 1748.
[92] Rubinstein SI. Big Data: The End of Privacy or a New Beginning? *International Data Privacy Law* 2013, 3(2): 74–87, 77.

relations on a global level provides deep insights into the identity and behavioural patterns of individuals.

3.3.3. Profiling

In addition, Big Data analytics enables the creation of highly detailed profiles of individuals based on their personal data. Analysing extensive datasets from various sources like social media, online transactions, and mobile devices makes it possible to uncover patterns and connections that reveal an individual's behaviour, preferences, and beliefs. Profiling identifies correlations and associations between data points, creating a rich and comprehensive view of the individual's digital persona. This level of profiling poses significant challenges to informational self-determination. The sheer amount and complexity of personal data being processed make it increasingly difficult for individuals to exercise control over their data, limiting their ability to manage their privacy and make informed decisions about how their data is used. This lack of control and transparency can lead to harmful outcomes, such as identity theft, discrimination, and exploitation.

3.3.4. Content Moderation

Another related constraint on informational self-determination arises from content moderation powered by Big Data processing tools. By analysing vast amounts of data, Big Data analytics can predict what products, services, and content individuals will likely to prefer, providing them with tailored recommendations and suggestions. These algorithms identify patterns and correlations between different data points, resulting in recommendations tailored to the individual's previous behaviour, preferences, and beliefs. While this personalised approach can be beneficial in delivering tailored experiences, it creates an echo chamber that reinforces existing beliefs and limits exposure to new ideas. As a result of limiting individuals' access to a diverse range of content and experiences, Big Data analytics continuously reduces autonomy and freedom of choice.

3.3.5. Automated Decision-Making

Finally, Big Data analytics raises an issue concerning automated decision-making, which relegates decisions about an individual's life—such as credit ratings, job prospects, and eligibility for insurance coverage or welfare benefits—to automated processes based on algorithms and artificial intelligence.[93] The use of Big Data intensifies automated decision-making by substantially improving its accuracy and scope. However, this reliance on data creates a dangerous situation where individuals have limited control over their personal data, and the algorithms used in automated decision-making can be prone to bias and discrimination. Because decisions based on data mining are mainly invisible to their subjects, significant issues arise around the right to reasoned decisions and the right to access to justice, as individuals are not aware of the basis or how the decision was made. Consequently, contesting and rectifying potential errors becomes increasingly challenging, further eroding the boundaries of informational self-determination.

The chapter demonstrates that the uses of Big Data analytics causes far-reaching privacy repercussions. It highlights numerous implications that undermined informational self-determination, including conflict between the users' intentions to share information, lack of access to personal data, facilitation of amassing information about an individual from multiple sources, limited access to a diverse range of content and experiences, questionable accuracy, and reliability of the underlying data (as depicted in Figure 2). Moreover, the analysis of these implications reveals that the issues at hand concern not only who has access to data but also the need for "technical control" to safeguard data from unauthorised use. As will be discussed in the next chapter, it is a core difference between the right to privacy and data protection. Therefore, if data protection is not to become lost in the conflation, there is a need to reconsider the interplay between the right to privacy and data protection. The challenge is how to decouple the two regimes to ensure the tenets of informational self-determination.

[93] Ibid.

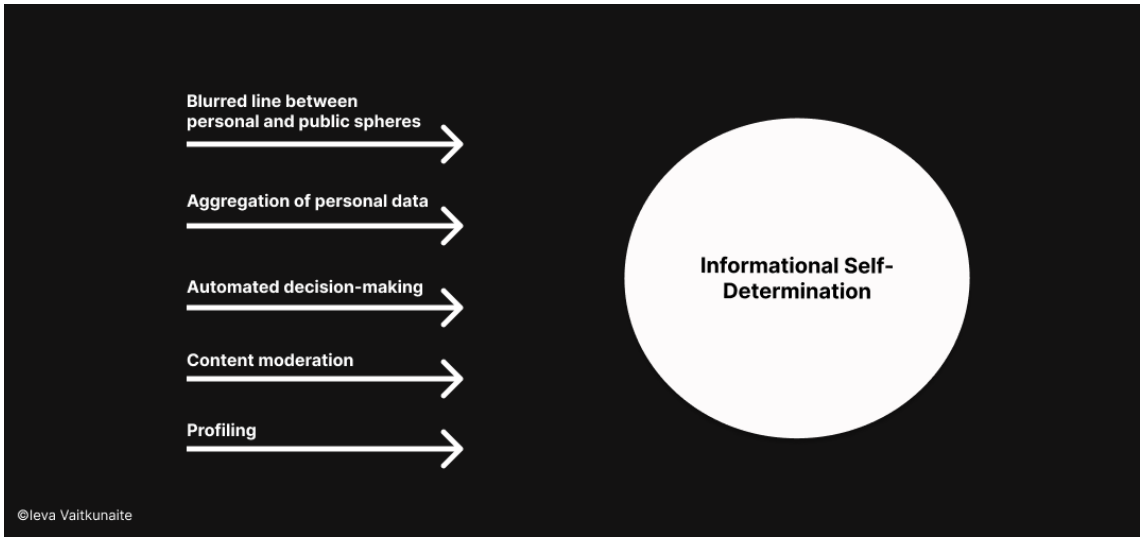

Figure 2 *The challenges posed to the boundaries of informational self-determination by the Big Data analytics*

4. RELATIONSHIP BETWEEN PRIVACY AND DATA PROTECTION

4.1. Defining the Relationship Between Privacy and Data Protection

As Big Data processing tools and technologies continue to advance, the use of personal data is becoming increasingly prevalent, and the need for privacy and data protection is more critical than ever. Although international human rights law recognises both privacy and data protection, there are ambiguities in distinguishing the two legal regimes. Therefore, it is crucial to establish clear distinctions between privacy and data protection.

4.1.1. Universal Character

The right to privacy is a human right, thus, has a universal character. It is protected under various international instruments, including Article 12 of the Universal Declaration of Human Rights[94] and Article 17 of the ICCPR.[95] It applies to all people regardless of nationality, race, gender, religion, or other characteristics.

The explicit recognition of data protection as a universal human right is lacking. As discussed in Chapter 2, the implementation of data protection laws is the responsibility of State parties. Indeed, some regional instruments have already recognised the right to data protection. For example, according to the CFREU,[96] data protection is a fundamental right on an equal footing with the right to private and family life. "Also, more and more national constitutions are amended with a separate right to data protection next to the more classical right to privacy."[97] From this point of view, the reinvention of data protection is ongoing, but simultaneously causes fragmentation at the international level. While the right to privacy has a universal character and explicit recognition as a human right under international law, data protection enjoys only fluctuating recognition.

[94] UN General Assembly, *Universal Declaration of Human Rights*, Resolution 217 A (III), 1948, Art. 12.
[95] UN General Assembly, International Covenant on Civil and Political Rights (1966) Treaty Series 999, Art. 17.
[96] EU, Charter of Fundamental Rights of the European Union (2012) 2012/C 326/02, Art. 8.
[97] Gutwirth S et al. (eds.), *Reinventing Data Protection?* Springer, Dordrecht, 2009, ix.

4.1.2. Goals and Objectives

The right to privacy and data protection have different goals and objectives. The right to privacy generally regulates access to information that concerns the private sphere of individuals, including their family life. It regulates who can collect, use, and disclose that information. In contrast, data protection rules do not necessarily distinguish between the private and public nature of the data. It concerns data processing: how it is collected, stored, used, and shared. One of the main objectives of data protection is to promote "fairness in the processing of data,"[98] including ensuring that individuals have control over their data and are aware of how it is being used. Data protection laws typically require organisations to obtain consent before collecting personal data, to limit the use and disclosure of that data to specific purposes, and to ensure that data is accurate and up to date. While there may be a slight overlap between the right to privacy and data protection, they have unique goals and objectives.

4.1.3. Application

The right to privacy generally refers to the right of an individual to control personal information and activities. It applies to areas considered private, namely, private life, family life, home, and correspondence. In contrast, data protection applies to the processing of personal data, the latter being understood broadly as "any information relating to an identified or identifiable natural person."[99] Data protection refers to the legal framework and measures in place to safeguard data, regardless of private or public nature of data. While the right to privacy applies to the private sphere, data protection does not distinguish between the privacy and public nature of data.

All in all, the relationship between data protection and privacy can be characterised by overlapping boundaries. Data protection is both narrower and broader than privacy. It is narrower because it only deals with the processing of personal data, whereas the scope of privacy is wider.[100] However, data protection is also broader because

[98] Bygrave LA. *Data Protection Law: Approaching Its Rationale, Logic, and Limits*. Kluwer Law International: The Hague/London/New York, 2002, 168.
[99] See, e.g., Council of Europe, Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data (1981) Treaty Series 108, Art. 2(a).
[100] Gellert R and Gutwirth S. The Legal Construction of Privacy and Data Protection, *Computer Law & Security Review* 2013, 29(5): 522–530, 526.

it encompasses the processing of personal data, even if it does not directly infringe upon privacy. On the other hand, privacy can be narrower and broader too. It may apply to the processing of non-personal data that still affects an individual's privacy, while it may not apply to the processing of personal data that is not considered to infringe upon one's privacy.

In conclusion, the right to privacy and data protection intertwine. Although data protection emerges as an offspring of privacy, it is carving its path as a distinct concept with its own goals and objectives. Data protection is essential to privacy laws because it provides a framework for ensuring that individual personal data is collected, processed, and used in a way that respects their privacy rights. "While privacy builds a shield around the individual, creating a zone of autonomy and liberty, data protection puts the activity of the processor in the spotlight, gives the individual subjective rights to control the processing of his/her personal data and enforces the processor's accountability."[101] Therefore, privacy and data protection are different but complementary. In order to devise an accurate and effective international privacy framework, they must remain sharply distinguished.

[101] Gutwirth S et al. (eds.), *Reinventing Data Protection?* Springer, Dordrecht, 2009, x.

5. RECOMMENDATION FOR A LEGAL REFORM

5.1. Advantages of Decoupling Privacy and Data Protection for Informational Self-Determination

An examination of international privacy regulations has revealed several normative gaps, including the lack of a clear distinction between privacy and data protection. Dividing these regimes and explicitly recognising the right to data protection as a human right would enhance the principles of informational self-determination. This argument presents several reasons, outlined below, to support its stance.

Firstly, a clear division between privacy and data protection would provide more legal certainty. As discussed, the two legal regimes have unique goals, objectives, and applications. However, there are many misconceptions about protected values and mistakes in blending unrelated zones of protection and using data protection and privacy interchangeably. Recognising the two as separate and independent regimes would improve precision in conflict resolution and the application of suitable remedies.

Secondly, recognising the right to data protection as a human right would ensure consistency in developing international privacy laws. The concept of informational self-determination necessitates that every individual is entitled to universal privacy and data protection. However, the right to data protection enjoys only limited recognition, it is not explicitly stipulated in the ICCPR but is established, for example, in the CFREU[102] and the case law of the ECtHR.[103] The European Union and the Council of Europe set a higher standard of data protection than the ICCPR. The current state of affairs of fragmented regional recognition of this right does not meet the standard of universality set by informational self-determination. Thus, the explicit recognition of the right to data protection next to the right to privacy in international law would be a logical step forward and guarantee universal protection of informational self-determination.

Similarly, decoupling privacy and data protection can allow for more comprehensive regulation of borderless privacy threats. At the European Union level,

[102] EU, Charter of Fundamental Rights of the European Union (2012) 2012/C 326/02, Art. 8.
[103] See, e.g., European Court of Human Rights, *Amann v Switzerland* (2000) Application No. 27798/95, para 65; European Court of Human Rights, *Rotaru v Romania* [Grand Chamber] (2000) Application No. 28341/95., para 43.

Article 3(2) of the General Data Protection Regulation[104] provides some extra-territorial application by extending the territorial reach beyond the European Union with two types of business activities: 1) offering goods or services to data subjects situated in the European Unions; and 2) monitoring of the behaviour of such data subjects. However, it is far from universal data protection regulation. Geographical borders do not limit privacy threats; thus, data protection must also be borderless. By separating privacy from data protection, governments and regulatory bodies could focus on creating and enforcing data protection regulations that address the unique challenges cross-border data flows pose. Ultimately, this approach can ensure that individuals are able to exercise greater control over their personal information, no matter where it is being processed or stored.

The recognition of data protection as a human right would set universal standards and restrictions on Big Tech corporations which have thus far operated in an unregulated digital landscape. Often, these corporations prioritise profit over individual privacy. By recognising data protection as a human right, governments and regulatory bodies could create a more level playing field and ensure that individuals have greater control over their personal information. Such recognition would address the power imbalances between Big Tech corporations and individuals, promoting fairness and equity in the digital realm.

Separating privacy and data protection could also address unregulated spaces at the intersection of privacy and data protection. A major obstacle lies in the aggregation of information without clear differentiations between private and public data. Such practices raise concerns about making correlations between seemingly innocuous data and making potentially harmful decisions about individuals. This lack of regulation poses a significant constraint on informational self-determination, as it limits the ability to control the collection and use of personal information. By decoupling privacy and data protection, it is possible to identify these gaps and establish mechanisms to address them effectively.

In conclusion, decoupling privacy and data protection and acknowledging data protection as a human right greatly enhance informational self-determination. Firstly, this separation provides clarity in resolving conflicts and filling the existing legal gaps at the

[104] EU, Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (2016) Official Journal of the European Union L 119, pp. 1–88.

convergence of privacy and data protection. Secondly, recognising data protection as a human right addresses the necessity for a universal framework and extends the protection of informational self-determination to an international scale. Lastly, it ensures more control over Big Tech corporations and enhances the empowerment of individuals within the digital realm.

5.2. New Approach to the Relationship Between Privacy and Data Protection

The findings presented in Section 2.3. has demonstrated that evolutive interpretation is useful to a certain level, but it has some limitations in addressing the rapid and transformative impacts of technological advancements. The proposed new approach does not aim to discard evolutive interpretation altogether, but rather to contextualise it within a theory that can better explain the underlying philosophy of technologies. Technological determinism is a theory that holds promise in reinforcing evolutive interpretation and advocating for more extensive legal reforms within the realm of international privacy law.

Technological determinism suggests that technology drives social change and that social systems and institutions, including law, must adapt to technological developments. It explores the role that technology plays in enabling societal progress. Technological determinism has two parts. "The first part is that technological developments take place outside society, independently of social, economic, and political forces."[105] Technologies or new products emerge from the activities of inventors, engineers, and designers following an internal, technical logic that has nothing to do with social relationships. "The more crucial second part is that technological change causes or determines social change."[106]

Technological determinism has the potential to bring about a shift in the interpretation of data protection. Currently, the concept of data protection is predominantly understood through the lens of privacy. However, it is problematic to interpret data protection merely as an offspring of the right to privacy. Drawing on

[105] Wyatt S. Technological Determinism is Dead; Long Live Technological Determinism. In Hackett JE et al. (eds.). *The Handbook of Science and Technology Studies*. Third Edition. The MIT Press: Cambridge, Massachusetts, 2008, 168.
[106] Ibid.

technological determinism, the thesis proposes a different perspective on the dynamics of interpreting privacy and data protection. The focus shifts towards considering data protection as a distinct focal point rather than solely focusing on its intersections with privacy. It is important to clarify that this viewpoint does not suggest that the two rights are unrelated. Privacy serves as an overarching concept that encompasses various aspects of data protection. It also does not imply that data protection has no added value. The argument, therefore, is that we should be able to evaluate data protection as a separate and fully developed right.

Figure 3 visually represents the differentiation between the current approach, which considers data protection as a subset of privacy, and the proposed new approach, which advocates for equal treatment of data protection and privacy. In the context of international privacy law, technological determinism may pave the way for a legal reform to address the privacy implications of new technologies such as Big Data analytics and ensure that privacy rights are protected effectively.

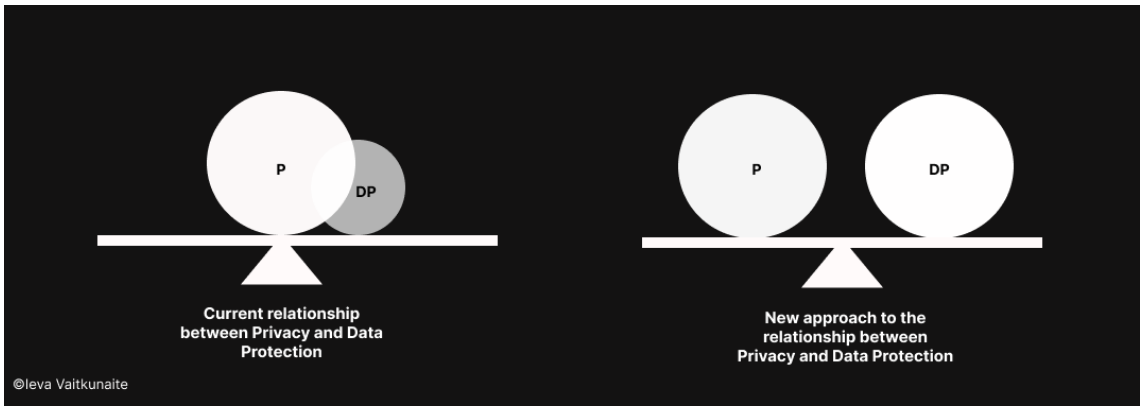

Figure 3 *The difference between the current and the new approach to the relationship between privacy and data protection*

5.3. Data Protection as a Distinct Human Right

Establishing the right to data protection as an independent human right with intrinsic value requires a coherent reconstruction. The proposed method for reform is based on the tripartite typology, the obligation of States to respect, protect, and fulfil and uses the fundamentals of Article 17 of ICCPR and General Comment 16. The reason for adopting this specific approach is that the tripartite typology offers a robust framework for developing human rights that are comprehensive yet specific, aligned with existing human rights standards, and oriented towards practical implementation.

As a starting point, the duty to respect implies that "States have a negative obligation not to take any measures that result in a violation of"[107] the right to data protection. Section 4.1.2. has discussed that data protection does not have a prohibitive character as its goal is to regulate the processing of data. This non-prohibitive characteristic prevents data protection from standing alone as an independent human right. Consequently, the right must identify instances where interference should be prohibited. Therefore, it should be reformed so that States shall not deliberately violate the right through their organs or agents. It must ensure that personal data is kept secure and protected from unauthorised access, theft, or misuse. Executive, legislative, and judicial branches of the State and other public or governmental authorities, at whatever level – national, regional, or local – should be in a position to engage the responsibility of the State party.[108]

Next, States must protect individuals from data protection violations. It means "that the State would need to proactively ensure that persons within its jurisdiction do not suffer from"[109] data protection violations at the hands of third parties. Aspects of the obligation to protect are already stipulated in General Comment 16 "[t]he gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law."[110] However, further development is necessary to require States to go beyond mere regulation and actively ensure "that persons are protected from any acts by private persons or entities that would impair the enjoyment of the"[111] right to data protection "to the extent that the Covenant rights are amenable to application between private persons or entities."[112]

Lastly, "the obligation to fulfil involves an obligation on States to adopt appropriate laws that implement their international undertakings."[113] This obligation

[107] Moeckli D et al. *International Human Rights Law*. Third edition. Oxford: Oxford University Press, 2018, 97.
[108] UN Human Rights Committee, *General Comment No. 31 [80]: The nature of the general legal obligation imposed on States Parties to the Covenant*, 26 May 2004, para 4.
[109] Moeckli D et al. *International Human Rights Law*. Third edition. Oxford: Oxford University Press, 2018, 97.
[110] UN Human Rights Committee, *CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, 8 April 1988, para 10.
[111] UN Human Rights Committee, *General Comment No. 31 [80]: The nature of the general legal obligation imposed on States Parties to the Covenant*, 26 May 2004, para 8.
[112] Ibid.
[113] Moeckli D et al. *International Human Rights Law*. Third edition. Oxford: Oxford University Press, 2018, 98.

directly aligns with the argument presented in Section 5.1., which posits that recognising the individual right to data protection can enhance legal certainty and precision in conflict resolution. To achieve this objective, the reform would require the inclusion of the right to data protection and corresponding remedies within domestic legislation. It entails legislative measures and the establishment of "judicial, administrative and educative and other appropriate measures, and an obligation to organise the structure of the state apparatus in a way that ensures the full exercise of"[114] a right to data protection.

Reconstructing data protection into a human right following the tripartite typology is a way to ensure the right functions positively and negatively. It means that it would not only regulate, channel, and control power but also prohibit its misuse. Consequently, data protection could strike a balance against conflicting interests without relying solely on the concept of privacy as a proxy. Reconstructing data protection in this manner makes it difficult to argue against its independent coexistence alongside the right to privacy.

5.4. Implementation of a Legal Reform

After establishing the content of the right to data protection, the next question emerges: how can it be effectively implemented? There are several ways in which the right to data protection could be recognised as a human right. The most desirable and straightforward option would be to amend the ICCPR to include data protection as a distinct human right explicitly. However, this would be a complex and time-consuming process, as it would necessitate the agreement of all signatory States to the treaty and could encounter political and legal challenges along the way.

Alternatively, another option could be the creation of a new protocol or treaty dedicated explicitly to safeguarding personal data as a human right. Some international organisations, such as the Council of Europe, have adopted this approach.[115] However, developing a new protocol or treaty would require substantial resources and strong political will. It could entail lengthy negotiations and ratification processes spanning several years.

[114] Ibid.

[115] In 1981, the Council of Europe adopted a separate Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (Convention No. 108) dealing with data protection as protection of the fundamental rights and freedoms of individuals, in particular, their right to privacy taking account of the processing of personal data relating to them.

The third and most viable option is updating General Comment 16. While the current version of General Comment 16 offers some guidance on data protection, it could be enhanced by explicitly acknowledging data protection as an independent human right. Through this update, the Comment could outline the positive and negative functions of the right to data protection, as well as articulate its content based on the tripartite typology. This approach avoids the lengthy negotiation process of amending the ICCPR or establishing a new protocol. Instead, it provides a concise framework that enables States to implement the right to data protection in practice effectively.

In conclusion, although amending the ICCPR or creating a new protocol would establish a legally binding framework for the right to data protection, these options are intricate and less immediately attainable. On the other hand, updating General Comment 16 presents a more practical and effective approach. This method would offer clear guidance to States, leveraging the advantages of soft law to establish the groundwork for recognising data protection as a human right. It provides a feasible pathway for advancing the recognition and protection of data protection in the short term.

6. CONCLUSION

After providing the analysis of the scope of the right to privacy, identifying its normative deficiencies, and addressing the practical complexities presented by Big Data analytics, it becomes evident that the evolutive interpretation fostered by the UN effectively adapts certain aspects of the right to privacy. However, it is insufficient in adequately upholding the right in the digital age and establishing universally applicable regulations. The ambiguity of evolutive interpretation has resulted in the increasing fragmentation between two intertwined legal frameworks – privacy and data protection – that do not fully guarantee informational self-determination. In light of these findings, the thesis draws the following conclusions:

Firstly, in terms of its benefits and shortcomings, evolutive interpretation has played a crucial role in enabling the right to privacy to evolve and remain relevant in the face of emerging digital challenges. It has facilitated the adaptation of privacy to changing societal contexts. However, a limitation of evolutive interpretation is its potential for digressive impact. It occurs when it inconsistently expands the scope of the right to privacy, deviating from the core values that underpin informational self-determination, such as human dignity and contextual integrity.

Secondly, the thesis established that Big Data analytics undermines the abilities of individuals to exercise informational self-determination. Big Data processing tools have opened new avenues for privacy violations that transcend national borders. Furthermore, the digital landscape, which lacks regulation over private actors and the pervasive privacy risks, actively demonstrates the limited prioritisation of privacy. These risks have translated into implications that diminish the boundaries of informational self-determination: 1) blurring the line between personal and public spheres; 2) aggregation of personal data; 3) enabling profiling of individuals; 4) limiting access to a diverse range of content and experiences; 5) intensifying automated decision-making.

Thirdly, the thesis has, thus, set forth a new approach to international privacy law: to decouple privacy and data protection and reconstruct data protection into a human right. The proposed approach aims to complement evolutive interpretation with the theory of technological determinism, which asserts that the law must adapt to keep pace with technological advancements. By adopting this approach, data protection can be

acknowledged as a distinct and autonomous human right rather than being interpreted solely as a subset of privacy regulations.

Accordingly, the thesis outlined the content of the right to data protection following the tripartite typology, i.e., the State's obligation to protect, respect, and fulfil. Through this reform, the right to data protection functions positively and negatively, ensures the balance with competing interests and exists independently of the privacy framework. Ultimately, the proposed solution has the potential to enhance the tenets of informational self-determination in many respects, as it would:

1. Provide legal certainty and clarity for individuals.
2. Harmonise international law and enable individuals to exercise informational self-determination, regardless of geographical boundaries or legal systems.
3. Repair the current power disbalance between Big Tech corporations and individuals.
4. Provide individuals with comprehensive regulation that would address sophisticated privacy threats.
5. Be more equipped to govern otherwise unregulated spheres at the intersection of privacy and data protection.

Finally, a fundamental challenge in the future will be the actual method of recognition of the right to data protection in international law. Since relying solely on evolutive interpretation is unlikely to bring about comprehensive reform in international privacy law, the thesis argued that a well-crafted update of General Comment 16 presents a more suitable and promising solution. The proposed soft law reform mapped on the tripartite typology would effectively equip the right to privacy and data protection to meet the evolving standards of informational self-determination in the digital age.

BIBLIOGRAPHY

BOOKS

1. Bignami F and Resta G. Human Rights Extraterritoriality: The Right to Privacy and National Security Surveillance. In Benvenisti E and Nolte G (eds). *Community Interests Across International Law*. Oxford University Press, 2018.
2. Bjorge E. *The Evolutionary Interpretation of Treaties*. Oxford University Press, 2014.
3. Bygrave LA. *Data Protection Law: Approaching Its Rationale, Logic, and Limits*. Kluwer Law International: The Hague/London/New York, 2002.
4. De Terwangne C. The Right to be Forgotten and Informational Autonomy in the Digital Environment. In Ghezzi A et al. (eds). *The Ethics of Memory in a Digital Age*. Palgrave Macmillan Memory Studies. Palgrave Macmillan, London, 2014.
5. Ishwara PB. *Idea and Methods of Legal Research*. Oxford University Press, 2019.
6. Keller H and Grover L. General Comments of the Human Rights Committee and their legitimacy. In Keller H and Ulfstein G (eds.), *UN Human Rights Treaty Bodies: Law and Legitimacy*. Cambridge: Cambridge University Press, 2012.
7. Kinfe Y. *Privacy and the Role of International Law in the Digital Age*. Oxford University Press, 2023.
8. Land KM and Aronson DJ (eds.). *New Technologies for Human Rights Law and Practice*. Cambridge University Press, 2018.
9. Moeckli D et al. *International Human Rights Law*. Third edition. Oxford: Oxford University Press, 2018.
10. Rouvroy A and Poullet Y. The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy. In Gutwirth S et al. (eds.), *Reinventing Data Protection?* Springer, Dordrecht, 2009.
11. Wyatt S. Technological Determinism is Dead; Long Live Technological Determinism. In Hackett JE et al. (eds.), *The Handbook of Science and Technology Studies*. Third Edition. The MIT Press: Cambridge, Massachusetts, 2008.

ACADEMIC JOURNALS

1. Bygrave LA. Data Protection Pursuant to the Right to Privacy in Human Rights Treaties. *International Journal of Law and Information Technology* 1998, 6(3): 247–284.
2. Gellert R and Gutwirth S. The Legal Construction of Privacy and Data Protection, *Computer Law & Security Review* 2013, 29(5): 522–530.
3. Gregorio De G and Radu R. Digital constitutionalism in the new era of Internet governance. *International Journal of Law and Information Technology* 2022, 30(1): 68–87.
4. Kokott J and Sobotta C, The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR, *International Data Privacy Law* 2013, 3(4): 222–228.
5. Ohm P. Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, *UCLA Law Review* 2010, 57: 1701–1777.
6. Rubinstein SI. Big Data: The End of Privacy or a New Beginning? *International Data Privacy Law* 2013, 3(2): 74–87.
7. Strauß S and Nentwich M. Social Network Sites, Privacy and the Blurring Boundary Between Public and Private Spaces, *Science and Public Policy* 2013, 40(6): 724–732.
8. Tzanou M. Data Protection as a Fundamental Right Next to Privacy? 'Reconstructing' a not so New Right, *International Data Privacy Law* 2013, 3(2): 88–99.

TABLE OF LEGISLATION

INTERNATIONAL TREATIES

1. Council of Europe, Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data (1981) Treaty Series 108.
2. Council of Europe, European Convention on the Protection on Human Rights and Fundamental Freedoms (1950) Treaty Series 5.
3. UN General Assembly, International Covenant on Civil and Political Rights (1966) Treaty Series 999.

4. UN, Statute of the International Court of Justice (1946) Treaty Series 993.
5. UN, Vienna Convention on the Law of Treaties (1969) Treaty Series 1155.

EUROPEAN UNION LEGISLATION

1. EU, Charter of Fundamental Rights of the European Union (2012) 2012/C 326/02.
2. EU, Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (2016) Official Journal of the European Union L 119, pp. 1–88.

UN RESOLUTIONS

1. UN Human Rights Council Resolution, The *right to privacy in the digital age,* A/HRC/RES/48/4, 2021.
2. UN General Assembly, *Universal Declaration of Human Rights*, Resolution 217 A (III), 1948.
3. UN General Assembly Resolution, *The right to privacy in the digital age,* A/RES/75/176, 2020.
4. UN General Assembly Resolution, *The right to privacy in the digital age,* A/RES/73/179, 2018.

UN GENERAL COMMENTS

1. UN Human Rights Committee, *CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, 1988.
2. UN Human Rights Committee, *CCPR General Comment No. 33: Obligations of States parties under the Optional Protocol to the International Covenant on Civil and Political Rights*, 2008.
3. UN Human Rights Committee, *General Comment No. 31 [80]: The nature of the general legal obligation imposed on States Parties to the Covenant*, 26 May 2004.

NATIONAL INSTRUMENTS

1. German Bundestag, Basic Law for the Federal Republic of Germany (1949) in the revised version published in the Federal Law Gazette Part III, classification number 100-1, as last amended by the Act of 28 June 2022.

TABLE OF CASES

AFRICAN COMMISSION ON HUMAN AND PEOPLE'S RIGHTS

1. African Commission on Human and People's Rights, *Centre for Minority Rights Development (Kenya) and Minority Rights Group International on Behalf of Endorois Welfare Council v Kenya* (2010) Communication 276/2003.

EUROPEAN COURT OF HUMAN RIGHTS

1. European Court of Human Rights, *Amann v Switzerland* (2000) Application No. 27798/95.
2. European Court of Human Rights, *Pretty v The United Kingdom* (2002) Application No. 2346/02.
3. European Court of Human Rights, *Rotaru v Romania* [Grand Chamber] (2000) Application No. 28341/95.
4. European Court of Human Rights, *Tyrer v United-Kingdom* (1978) Application No. 5856/72.

GERMAN FEDERAL CONSTITUTIONAL COURT

1. German Federal Constitutional Court, *Order of the First Senate* (1983) 1 BvR 209/83, paras 1-214.

INTER-AMERICAN COURT OF HUMAN RIGHTS

1. Inter-American Court of Human Rights, *Bámaca-Velásquez v Guatemala* (2000) Judgement C Series No. 70.
2. Inter-American Court of Human Rights, *The Gómez-Paquiyauri Brothers v Peru* (2004) Judgement C Series No. 110.
3. Inter-American Court of Human Rights, *The Mayagna (Sumo) Awas Tingni Community v Nicaragua* (2008) Judgement 136 International Law Reports 73.

INTERNATIONAL COURT OF JUSTICE

1. International Court of Justice, *Dispute regarding Navigational and Related Rights (Costa Rica v Nicaragua)* (2009) Judgement I.C.J. Reports.

UN HUMAN RIGHTS COMMITTEE

1. UN Human Rights Committee, *Antonius Cornelis Van Hulst v Netherlands* (2004) Communication No. 903/1999, U.N. Doc. CCPR/C/82/D/903/1999.
2. UN Human Rights Committee, *Coeriel and Aurik v Netherlands* (1994) Communication No. 453/1991, U.N. Doc. CCPR/C/48/D/453/1991.
3. UN Human Rights Committee, *Francis Hopu and Tepoaitu Bessert v France* (1997) Communication No. 549/1993, U.N. Doc. CCPR/C/60/D/549/1993/Rev.1.
4. UN Human Rights Committee, *H.S. v Australia* (2015) Communication No. 2015/2010, U.N. Doc. CCPR/C/113/D/2015/2010.
5. UN Human Rights Committee, *I. P. v Finland* (1993) Communication No. 450/1991, U.N. Doc. CCPR/C/48/D/450/1991.
6. UN Human Rights Committee, *Khaoukha Marouf v Algeria* (2014) Communication No 1889/ 2009, U.N. Doc. CCPR/C/110/D/1889/2009.
7. UN Human Rights Committee, *Nabil Sayadi and Patricia Vinck v Belgium* (2008) Communication No. 1472/ 2006, U.N. Doc. CCPR/C/94/D/1472/2006.
8. UN Human Rights Committee, *Roger Judge v Canada* (2003) CCPR/C/78/D/829/1998.
9. UN Human Rights Committee, *Toonen v Australia* (1994) Communication No. 488/1992, U.N. Doc CCPR/C/50/D/488/1992.