African Journal on Privacy & Data Protection

To cite: D Sato 'Modern problems require modern solutions: Data protection and the right to privacy in national social support programmes in Malawi' (2024) 1

African Journal on Privacy & Data Protection 119-151

Modern problems require modern solutions: Data protection and the right to privacy in national social support programmes in Malawi

*Daniel Sato**
Lawyer, Malawi

Abstract:

The right to privacy is a basic right, which is closely associated with the right to dignity. The piloting of information processing technology has heightened the risks associated with information processing, therefore presenting a modern problem. In Malawi, the government through the Department of Economic Planning collects mammoth personal information used in social support programmes through a framework termed the Universal Beneficiary Registry. The information is used by the government and various social support partners. The article notes that this information is disposed to various risks, possibly violating the right to privacy of an individual or a group of individuals. The article investigates the safeguards that are there under the Unified Beneficiary Registry for the protection of the right to privacy. It concludes that the Unified

* BA; LLB (Malawi); satochikondi@gmail.com. At the time of writing and submitting this paper, the only comprehensive law on data protection in Malawi, the Data Protection Bill of 2021, remained in draft form. However, at the time of publishing, the Data Protection Bill had been passed into law having been introduced as Bill No 22 of 2023. The bill has been assented to by the President and is now the Data Protection Act. Once gazetted, it immediately or on the date appointed in the gazette becomes part of the Laws of Malawi.

Beneficiary Registry has taken reasonable steps to safeguard the data that it holds through technical and organisational measures. Regardless, it is opined that lack of a comprehensive legal regime on data protection might impact efforts to protect data under the UBR in Malawi. The article recommends that the area of data protection/privacy law needs urgent reform to address these contemporary problems.

Key words: privacy; data; data protection; Unified Beneficiary Registry; MNSSP II

1 Introduction

The evolution of advanced information and communication technologies has streamlined the collection of extensive amounts of personal data. Personal data is increasingly collected, generated, stored and utilised by institutions both in the public and private sector. Collected data is utilised in the provision of healthcare, health and other types of insurance, education, banking and financial services and hospitality services. Information technologies (Its) have also enabled the assortment of personal data in the delivery of social programmes.

When it comes to National Social Support Services (NSSPs),[1] information and communication technologies are now used to collect and store information about people for development programmes.[2] This serves various purposes such as targeting of beneficiaries in national social support programmes and has various benefits such as the avoidance of duplication of efforts.[3] It allows various players in NSSPs to have critical data that helps in decision making based on areas of need, among some motivations.

The article's focus borders on data collected by the government for National Social Support Programmes (NSSPs) under the Unified Beneficiary Registry (UBR) framework in Malawi.[4]

Until recently, Malawi lacked a legal framework to address data protection and privacy issues. There has been a marked shift with the adoption of laws that

1 The Malawi National Social Support Programme is an initiative aimed at strengthening social support and social protection to persons whose living standards are vulnerable. It currently is in its second phase and the focus under this second phase is partly integration through linkages, concerted monitoring and strengthened systems including data collection and management systems; Malawi National Social Support (MNSSP II), March 2018. Also see https://socialprotection.org/discover/legal_policy_frameworks/malawi-national-social-support-programme-mnssp-ii (accessed 15 September 2023).

2 B Wagner & C Ferro 'Data protection for social protection: Key issues for low- and middle-income countries' Working paper for the GIZ (Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ)) GmbH.

3 As above.

4 The UBR is a database used by various social support programmes in Malawi. Its core function is to provide a single source of data and data processing for various social protection programmes. It allows various social protection players to target their beneficiaries. It was introduced in 2016. See https://www.impactpool.org/jobs/737267 (accessed 20 September 2023).

seek to protect personal data of individuals.[5] For organisations that bothered to have data policies, they organised their data policies in ways that fit their thinking of data protection and privacy. Nevertheless, in the past years there has been a surge in legislative attention in this domain.[6] These include the enactment of the Electronic and Cyber Security Act and the drafting of the Data Protection Bill signifying a contribution to data protection as well as a marked growth of interest in this realm.

Among these progresses and the intensifying expansion of data collection and processing, the government introduced the Unified Beneficiary Registry (UBR).

2 Unified Beneficiary Registry

The UBR is a centralised database. Under it, the government in collaboration with various development partners collects data about human targets for various development programmes.[7]

The primary role of the UBR is to support targeting of households with potential interventions that are likely to have a positive outcome on their day-to-day livelihood.[8]

The UBR collects and stores data to enable programme planners and implementers in social protection programmes to target households more efficiently and effectively using information and communication technology services.[9] Furthermore, the UBR offers an interface for access, exploiting and sharing data based on the specific requirements of the discrete social protection programmes.[10]

As additional data continues to be collected under the UBR, the amount of (sensitive) information on the table of risk against manipulation increases and so does the risk for unauthorised access, accidental damage and disclosures among some. Also, with ongoing developments in information and communication technology, problems concerning the right to privacy emerge. This article highlights the need for modern solutions to address these potential risks on violation of the right to privacy.

5 J Kainja 'Privacy and personal data protection: Challenges and trends in Malawi' (CIPESA September 2018), https://cipesa.org/?wpfb_dl=300 (accessed 23 August 2022).
6 As above.
7 https://www.ubr.mnssp.org/?page_id=2 for information on the Universal Beneficiary Registry (accessed 23 August 2021).
8 Kainja (n 5).
9 UBR (n 4).
10 As above.

The initiation of data-driven technologies and data sharing between many entities gives rise to a range of legal complexities.[11] Some of the issues of interest in data and data management include privacy of data subjects and data sharing; breaches of related obligations in a data exchange or access transaction; data sharing obligations; data sharing agreements (DSAs); and liability in cases of breach.

The subject of privacy protection has evolved over the years. In the digital era, privacy laws and regulations have risen to prominence largely because of the simplicity with which data collection, keeping and transmission are done and, therefore, potential risks accmpanying it. Traditionally, the right to privacy is not an easily-defined concept owing to various social factors and expectations of the self, which sometimes blur the lines on where privacy must start and end.

Prior to the seminal article 'The right to privacy' by Warren and Brandeis,[12] there was limited discourse within academic circles regarding the right to privacy and the inevitability for data protection to safeguard the interests of data subjects. The notion of privacy now is possibly well-established. Nonetheless, it becomes more complicated with the dawn of digital technologies.

Before the introduction of information technologies, details of individuals were collected and recorded on paper. Solove notes that details of individuals were easily forgotten and destroyed by the collectors.[13] Still, the advent of information technologies has enhanced opportunities for public and private organisations to process personal data, enabling data retention easily without the limitations of physical storage space. As Clarke notes, this poses various risks,[14] as noted earlier.[15]

Additionally, it would thus be argued that digital technologies have made it easier to transact in data with remarkable risks due to the faith entrusted to a single controller. Once data is collected and stored in a database, more control essentially is given to the controller.

In addition to the risks associated with data collection espoused above, the problem of lack of knowledge of data flows by a data subject and blacklisting also becomes apparent once data is transferred into a database such as the UBR.[16]

11 AB Makulilo (ed) *Law, governance and technology series: African data privacy laws* (2016).
12 SD Warren & LS Brandeis 'The right to privacy' (1890) 4-5 *Harvard Law Review* 193-195; it is a work of note on the history of the right to privacy with vast scholarly recognition.
13 DJ Solove 'Conceptualising privacy' (2002) 90 *CLR* 1088.
14 R Clarke 'Information technology and datavaillance' (1988) 31 *Communications of ACM* 505-508; see also AM Froomkin 'The death of privacy?' (2000) 52 *Stanford Law Review* 1472. The risks intimated include lack of knowledge of potential uses, dangers of stalking and discrimination by governments.
15 Warren & Brandeis (n 12).
16 Clarke (n 14).

Empirically, the case of Bodil Lindqvist v Åklagarkammaren i Jönköping[17] provides a classic example of data protection breaches. In this case, sensitive health data of individuals was exposed on the internet. It can be comprehended, therefore, that the UBR is not intrinsically insusceptible to possible risk of unauthorised access or disclosures of the data it contains. Effects of data breaches can cost information holders a fortune. Mobile communications giant T-Mobile has been on the receiving end of consequences of data breaches wherefrom it was forced to settle a claim centering around 'unauthorised access' to a section of customer data that was put up for sale on a known cybercriminal forum.[18]

With these fears based on technological advances, the legal response has been to enact data protection legislation. Whereas data protection laws have been enacted in other jurisdictions, and are used to regulate data processing, including the imposition of fines, as in the T-Mobile case, other countries such as Malawi are yet to implement robust legal systems to address these fears.

Whereas it will be seen that technology has largely played a part in data protection laws, Bygrave expands on other catalysts for the advent of data protection laws.[19]

Bygrave explores three primary influences driving the development of data protection laws.[20] First, he attributes technological evolution and related trends as a key driver for devising of data protection laws. Under this category, Bygrave highlights that growing volumes of stored data and its cross-border sharing have created a demand for safeguards to protect personal data. The second driver is attributed to increased public fears relating to privacy and multifaceted principles relating to data protection. Lastly, Bygrave notes that the interest developed by international legal instruments has influenced a proliferation of data protection laws in domestic and other international dispensations.

Nevertheless, in 2004 Bygrave expanded his drivers to embrace philosophical aspects, distinguishing them as indispensable in determining the levels of privacy within a given society.[21] Under this conception, privacy is tied to value systems of each individual society. For instance, Bygrave notes that societies with liberal ideas are more likely to exhibit a higher concern for privacy.

17 ECJ Case C-101/01; AB Makulilo 'Does the Lindqvist decision by the ECJ make sense in terms of its treatment of the application of art 25 of Directive 95/46/EC to uploading and downloading of personal information on internet homepages? Tutorial Paper, cm, Norwegian Research Centre for Computers and Law (NRCCL) 2006.

18 https://www.csoonline.com/article/567531/the-biggest-data-breach-fines-penalties-and-settlements-so-far.html (accessed 20 September 2023).

19 LA Bygrave 'Privacy and data protection in an international perspective' (2010) 56 *Scandinavian Studies in Law* 175.

20 As above.

21 As above.

Nevertheless, whatever the philosophical thinking behind data protection might be, it can only be argued that technological advancements are the major catalyst for privacy laws.

Unregulated data processing has the potential to result in human rights violations, including infringements on the rights to privacy, dignity, security of the person, property and to be free from discrimination without lawful excuse.[22] Unregulated data processing has also been feared to pose identity theft,[23] harassment and stalking,[24] as well as targeting risks, among other risks.[25] The T-Mobile case study above clearly illustrates that personal data may be of immense interest to criminals.

This article analyses the extent to which the UBR framework, the largest of any data processing scheme in Malawi (apart from compulsory civil registration), protects personal data of its subjects in its processing and sharing framework, in line with domestic and international data protection law.

The article employs a desk research methodology and adopts the UBR's data management and sharing protocols as a reference point for analysis for data protection laws in Malawi. The underlying assumption is that the UBR falls short from adequately safeguarding the right to privacy of data subject, primarily attributed to the lack of a definite and robust legal framework for personal data protection in Malawi.

3 UBR in context

Prior technical assessment has shown that the UBR is prone to risks such as the lack of a firewall to guard against intrusion.[26] This has the potential of invading data subjects' privacy. Prior legal assessment of the UBR does not exist in the

22 G Sartor 'Human rights in the information society: Utopias, dystopias and human values' in M Viola de Azevedo Cunha and others (eds) *New technologies and human rights: Challenges to regulation* (2013) 14-24; P Ferreira 'Angels and demons: Data protection and security in electronic communications' in M Viola de Azevedo Cunha and others (eds) *New technologies and human rights: Challenges to regulation* (2013) 203-216.

23 See generally E Aimeur & D Schonfeld 'The ultimate invasion of privacy: Identity theft' Ninth Annual International Conference on Privacy, Security and Trust 2011, www.site.uottawa.ca/~nelkadri/CSI5389/Papers/8-Aimeur_and_Schonfeld_PST2011.pdf (accessed 22 August 2021).

24 S Sissing & J Prinsloo 'Contextualising the phenomenon of cyber stalking and protection from harassment in South Africa' (2013) 2 *Acta Criminologica: Southern Africa Journal of Criminology* 15, 19-20.

25 Eg, China is using technology to monitor, control and target people. See X Qiang 'Dataveillance' in Xi Jinping's Brave New China" *Power 3.0* 26 April 2018, www.power3point0.org/2018/04/26/dataveillance-in-xi-jinpings-brave-new-china/ (accessed 22 August 2021); S Feldstein 'The road to digital unfreedom: How artificial intelligence is reshaping repression' (2019) 30 *Journal of Democracy* 40-45.

26 K Lindert and others 'Rapid social registry assessment: Malawi's Unified Beneficiary Registry', https://openknowledge.worldbank.org/handle/10986/31012 31 (accessed 18 October 2021).

public sphere and the UBR being a relatively modern project, not much research has been done surrounding its legal implications.

Additionally, elsewhere prior research on data processing provides thorough views on privacy, data management and the risks of information processing, hence requiring protection.[27] In Malawi, these views are largely wanting owing to the absence of extensive prior research in this area. Yet, a researcher has explored this field through her Master's thesis, focusing on the right to data privacy for individuals in underprivileged societies.[28] Her hypothesis centres on the concept that socio-economic experiences amplify the risks and instances of violations concerning the right to privacy and data protection.[29]

As alluded to, this article employs a legal audit approach on the UBR. Relatively, data privacy is a whole new area in Malawi. As at the time of writing this article, the primary endeavour toward a data protection law was still in draft format, personified in the Data Protection Bill. This position is in contrast to the time of the previous study steered by Nyemba.[30] Additionally, unlike the previous study, this study focuses on a practical setting and seeks to analyse the intersection of the law and practice in the workings of the UBR. With an ambitious project such as the UBR and, potentially, other projects, it is pertinent to study the status of the law providing for data protection in Malawi as it meets practice.

4 A research framework

The perceptions of privacy and data protection are crucial to any study in the domain of the right to privacy in digital technologies.

27 Makulilo (n 11). Makulilo studies the status of data protection in sub-Saharan Africa. He appreciates the need to protect personal data but concludes that the regulatory scheme is still in its infancy in most sub-Saharan countries.

28 C Nyemba 'Right to data privacy in the digital era: A critical assessment of Malawi's data privacy protection regime' GC Publications, 2018/2019, https://repository.gchumanrights.org/bitstream/handle/20.500.11825/1829/Nyemba%20HRDA.pdf?sequence=1&isAllowed=y (accessed 22 August 2021).

29 As above.

30 As above.

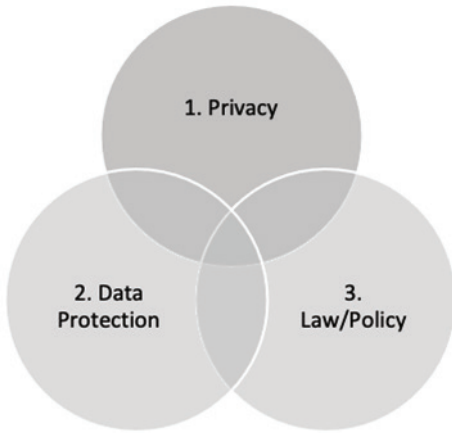

Figure 1: Article's thematic concepts

There arguably are various contested concepts of data protection and privacy.[31] To better understand the challenges surrounding data protection and privacy concepts, the article proceeds to elucidate the main thematic concepts as well as the manner in which they relate to one another. Conceptually, the understanding in this article is that data protection is a resultant concept that is used to guarantee privacy of the subjects to which data relates. Figure 1 presents the thematic concepts of the article and their intersection with the law.

From figure 1, the guiding understanding is that the concept of data protection itself is guided by privacy considerations. The right to privacy; and the concept itself, largely inform the need for data protection. Data protection in its entirety is a legal and policy mechanism that ensures privacy of individuals to which data relates. Nonetheless, a caveat must be stated at the outset that data protection is not entirely about the right to privacy.[32] Data protection may be achieved through legal and policy mechanisms.

4.1 Privacy, a jurisprudential term?

Privacy as a legal concept is a contested term.[33] Outside legal scholarship, the conception of privacy is also largely relative to various social and cultural phenomena. As Young eloquently argued, 'privacy is like an elephant; it is more

31 DK Mulligan, C Koopman & N Doty 'Privacy is an essentially contested concept: A multi-dimensional analytic for mapping privacy' (2016) *Philosophical Transactions of the Royal Society A 374.*

32 C Kuner 'An international legal framework for data protection: Issues and prospects' (2009) 25 *Computer Law Security Review* 308.

33 Mulligan (n 31).

readily recognised than described'.[34] This implies that the concept of privacy is subjective and can mean different things to different individuals.[35]

As illustration, Mr X may not have a problem sharing his address with the public. Therefore, he would not have problems with settings on social media platforms that display his address. Mr X's wife, on the other hand, considers her address very private information. She would consider such details amenable to decisional privacy. This illustrates the simple but delicate issue of privacy being a relative and contested concept.

What, then, is the essence of the notion of privacy? By tradition, the right to privacy or to one's person was conceived as the right to be free from interference or intrusion, to be left alone.[36] In this setting, the expression 'right to privacy' does not denote a legal requirement for privacy but rather signifies the individually-abstracted need to be left alone. Privacy as the right to be left alone was popularised by the American authors Warren and Brandeis.[37] Unpacking the idea that the person has an entitlement to be let alone essentially is accepting the notion that the person has some immunity from interference, subject to other lawful overriding interests that may be sought over this immunity by the state or authorised private actors. Such lawful interests would be social security, as in the case of the UBR. However, the qualification is that for privacy interference, the same must be lawful. It would be argued that this extends to the processes after the initial privacy disruption.

The traditional conception of privacy is narrow in modern dispensation. It arguably sets off from an understanding that every individual has personal confines that must not be accessed without the person's consent. Perturbed by the arguably waning conception of privacy, Westin was among the first scholars to attempt a reformulation of the concept of privacy.[38] Westin articulated privacy as 'the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others'.[39]

Westin's definition assumes that the determination of privacy question invariably is within the discretion of the individual in question and, thus, leaning towards decisional privacy. However, such a conception would seem to be inconsistent with the term 'privacy' itself and renders the term, as earlier feared, subject to inconsistences of application. The definition of privacy should extend to the claims that the law may also impose. Nonetheless, Neethling appears to

34 C Goodwin 'Privacy: Recognition of a consumer right' (1991) 10 *Journal of Public Policy and Marketing* 149.
35 AR Miller 'The assault on privacy: Computers, data banks, and dossiers' (1971) 22 *Case Western Reserve Law Review* 808; also see Goodwin (n 34).
36 R Allen & A Turkington *Privacy law: Cases and materials* (2002).
37 Warren & Brandeis (n 12) 193.
38 As above.
39 As above.

agree with Westin, stating that the self-determination of interests in information is the fundamental basis of an individual's privacy.[40]

Even so, the overarching tenet in the conception of privacy is that, therefore, there is a will to exclude certain information from publicity. This research adopts the approach that privacy encompasses both decisional, legal and policy interests.

5 Theoretical underpinnings

5.1 Information control theory

One of the most well-known theories of privacy is the information control theory. Westin's classical privacy theory is of particular illumination. The information control theory has two main propositions. The initial assumption is that individuals possess control over their personal information concerning data controllers or data processors. The second assumption, as a substitute to the first, suggests that individuals can potentially impact the information practices of data related to them.

According to Westin's theory, 'privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others'.[41] The sentiments in Margulis's conception of information control echo those of Westin. Margulis states that 'privacy, as a whole or in part represents control over transactions between person(s) and other(s), the ultimate aim of which is to increase autonomy and or to minimise vulnerability'.[42]

The information control theory has several variants. Tavani has attempted to provide a summary of some of these variants:

> According to Fried, privacy 'is not simply an absence of information about us in the minds of others, rather it is the control over information we have about ourselves' (1990, 54). Miller embraces a version of the control theory when he describes privacy as 'the individual's ability to control the circulation of information relating to him' (1971, 25). A version of the control theory is also endorsed by Westin ... and Rachels appeals to a version of the control theory of privacy in his remarks concerning the connection between 'our ability to control who has access to information about us and our ability to create and maintain different sorts of relationships' (1995, 297).[43]

40 J Neethling 'The concept of privacy in South African law' (2005) 122 *South African Law Journal* 18.
41 AF Westin *Privacy and freedom* (1967) 7.
42 ST Margulis 'privacy as a social issue and behavioural concept' (2003) 59 *Journal of Social Issues* 245.
43 HT Tavani 'Philosophical theories of privacy: Implications for an adequate online privacy policy' (2007) 38 *Metaphilosophy* 3, cited and critiqued in Makulilo (n 11).

The information control theory, as observed by Makulilo, faces criticism.[44] The primary objection is that the theory erroneously assumes that privacy inevitably is intrinsically affected when an individual discloses information. I respectfully disagree. A person does not necessarily lose privacy when they no longer have control; their privacy is only made vulnerable. Additionally, the loss of control also essentially reduces their autonomy, as duly noted by Margulis.[45] This critique is further refuted by Davis who maintains that the relinquishment of control does not equate a loss of privacy. Consequently, privacy may be compromised even when control has not been fortified.[46] In effect, the theory advocates greater information control by the subject.

The criticism mentioned above leads to another critique of the information control theory, highlighting its failure to segregate between actual and potential violation of privacy.[47]

Despite the criticisms levelled against the information control theory, it is measured as one of the most directly applicable theories to address issues related to data processing by organisations.[48] The information control theory also aligns with the fundamental principles of data protection law, emphasising increased involvement of data subjects, including their ability to influence the processing of information about themselves.[49] Additionally, the theory imparts significant regulatory influence to the concept of privacy, enabling advocates of data protection law to explore the principled dynamics and self-determination involved data processing.[50]

The information control theory and its propositions will be employed to analyse whether data protection law in Malawi offers and enables information control by data subjects to ensure data protection of data subjects.

5.2 Pragmatism theory

The major proponent of this theory is Solove.[51] He advocates a bottom-up approach in dealing with privacy issues. His approach basically is that privacy issues must be looked at pragmatically. In essence, this postulation is that the law must provide room for analysing privacy considerations in the context in

44 Makulilo (n 11).
45 Margulis (n 42).
46 S Davis 'Is there a right to privacy?' (2009) 90 *Pacific Philosophical Quarterly* 451.
47 D Elgesem 'The Structure of rights in Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of such Data' (1999) *Ethics and Information Technology* 290; R Volkman 'Privacy as life, liberty, property' (2003) 5 *Ethics and Information Technology* 203.
48 LA Bygrave 'The place of privacy in data protection law' (2001) 24 *University of New South Wales Law Journal* 282.
49 As above.
50 As above.
51 DJ Solove 'Introduction: Privacy self-management and the consent dilemma' (2013) 126 *Harvard Law Review* 1879, 1880.

which they occur. Privacy, in his view, is not a concept that can apply universally to different situations. Solove's bottom-up approach calls for an understanding of privacy from scenario-specific circumstances such as a disruption of practices, disturbance of peace of mind, among possible situations.[52] In examining the practices under the UBR, it is important to analyse whether in the context of the law, the UBR's practices offer pragmatic responses to data protection. One of the ways in which to assess this in Solove's lens is whether data subjects can still be said to have control over their personal information.

The pragmatism theory can be said to agree with the conception of data protection as postulated by De Hert and Gutwirth who note that data protection is a necessity on the assumption that that private and public actors need to be able to nonetheless use personal information because it benefits the society. The conception therefore is that data protection is not a means to prevent data processing, but a vehicle to promote justifiable data processing[53].

The pragmatism theory is not without criticism. One of the major criticisms is that it renders itself to so much subjectivity rendering the safeguard of privacy in the balance by promoting vagueness and ambiguity in the conception of privacy[54]. However, it is argued that this subjectivity may be controlled by means of legislative ingenuity that seeks to control data processing practices, while giving room for data processors to make privacy choices in the confines of a particular regulatory environment. For instance, one way of achieving this is requiring data processors to disclose reasons for the actions that they take in regard to the data that they process. Another criticism to the pragmatism theory is that regardless, the legislature would need to have a working concept of privacy to better define the parameters in which it applies. The critics argue that divorcing the understanding of privacy from any theory is to argue in circles.[55]

Regardless of the criticisms, the pragmatic theory provides explanations of legislative practices and the different approaches taken in tackling the question of privacy. In this regard, it is important as it helps to analyse whether the legal environment in data protection in Malawi is flexible to accommodate various privacy questions. Additionally, it will be useful to analyse whether it gives room to data processors to address privacy questions based on the understanding that data processing is inevitable nonetheless, more specifically, and in relation to the study objectives and whether or not Malawi's municipal laws are based on pragmatic considerations.

52 As above.
53 As above.
54 DK Mulligan 'Privacy is an essentially contested concept: a multi-dimensional analytic for mapping privacy(, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5124066/ (accessed 14 February 2024)
55 A Thierer 'Book review: Solove's *Understanding Privacy*' (2008) *The Technology Liberation Front* https://techliberation.com/2008/11/08/book-review-soloves-understanding-privacy (accessed 14 February 2024)

6 Modern problems require modern solutions: A juxtaposition of data protection in relation to the right to privacy

Data protection laws are increasingly being adopted world over in response to concerns and problems of privacy invasion through data processing. This partially is attributable to the easiness in record keeping, which further accelerates risks associated with access and disclosure of information, among others.[56]

The term 'data protection' is regarded as having originated from the German term *datenschutz*.[57] Under this etymological conception, data protection is understood as the relationship between the collection and dissemination of data, the use of technology or other means and the public expectation of privacy, as well as the legal and political (and policy) issues surrounding them.[58] At its core, data protection in the sphere of pragmatism accepts that data about individuals has to be used but being cautious with the need to safeguard an individual's privacy preferences and personally identifiable information.[59]

Bygrave notes that data protection need not always involve legal measures.[60] Indeed, as noted by Michael and others,[61] there are various parameters to data protection, which include political, social and public expectations of privacy, among others. Bygrave thus describes data protection as deliberate legal and non-legal procedures undertaken to safeguard data subjects from detriment that may result from data processing of data about themselves. He further understands it to include the various philosophies, values and ethics attached to data processing.[62]

As noted by Michael and others,[63] data protection also encompasses societal understanding of the term itself. One of the most noted socio-definitions of data protection is Podlech's 1976 definition that (data protection) is 'promulgating and adopting conditions for data processing in a particular society, to meet acceptable standards in that particular society'.[64]

It is thus argued that data protection encompasses the legal and policy safeguards of a person's privacy (throughout referred to as the data subject) with regard to the processing of data concerning themselves by another person or institution.

56 Bygrave (n 17).
57 MG Michael *Uberveillance and the social implications of microchip implants: Emerging technologies* (2014).
58 As above.
59 V Torra *Introduction, data privacy: Foundations, new developments and the big data challenge* (2017) 1-21.
60 Bygrave (n 48).
61 Makulilo (n 11).
62 UBR (n 4.)
63 Makulilo (n 11).
64 A Podlech. *"Gesellschaftstheoretische Grundlage des Datenschutzes." In Datenschutz und Datensicherung,* edited by R Dierstein, H Fiedler, and A Schulz, 311- 326. Köln: J. P. Bachem Verlag.

The right to privacy is a fundamental human right recognised as such by various international instruments, including the Universal Declaration of Human Rights (Universal Declaration) and the International Covenant on Civil and Political Rights (ICCPR). It has been touted as a fundamental value of legal protection by the Australian Law Commission.[65] Article 17 of ICCPR, to which Malawi is a party, provides:

> (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.[66]

In relation to data protection, Kuner argues that privacy is a concept that is independent from data protection although the former should be considered more broadly. Kuner nonetheless acknowledges that there is a significant synergy between the two concepts, with privacy considerations being considered a vital driving force behind data protection practices and requirements.[67]

Despite there being an overlap between the two concepts, the question that normally is asked is whether privacy and data protection are one and the same thing. Cuijpers[68] raises this question and answers in the negative, concurring with Block that privacy and data protection essentially are different.[69] The two argue that since an individual's right to privacy safeguards an undisturbed private life and offers the individual control over intrusion of the private sphere, it is different from protection of the individual with regard to the processing of personal data, which is not restricted to the private sphere of the individual.[70]

Makulilo makes a very insightful observation in his doctoral thesis. He notes that regardless of the fact that scholars continue to argue that although clearly engrained in privacy protection, *data protection* does not necessarily exclusively raise *privacy* issues.[71] De Hert and others argue that the concept of privacy involves prohibitive rules that require 'don'ts', whereas the concept of data protection includes rules that organise and control the way personal data can only be legitimately processed if some conditions pertaining to the transparency of the

65 https://www.alrc.gov.au/publication/serious-invasions-of-privacy-in-the-digital-era-dp-80/2-guiding-principles/principle-1-privacy-is-a-fundamental-value-worthy-of-legal-protection/ (accessed 22 March 2022).
66 International Covenant on Civil and Political Rights (ICCPR) 999 UNTS 171 art 17.
67 C Kuner 'An international legal framework for data protection: Issues and prospects' (2009) 25 *Computer Law and Security Review* 308.
68 C Cuijpers 'A private law approach to privacy: Mandatory law obliged?' (2007) 4 *SCRIPTed* 312.
69 Makulilo (n 11).
70 As above.
71 Makulilo cites P de Hert & E Schreuders 'The relevance of Convention 108' 33 42 Proceedings of the Council of Europe Conference on Data Protection, Warsaw, 19-20 November 2001, cited in 'EU study on the legal analysis of a single market for the information society', November 2009, ch 4, 4.

processing, the participation of the data subject and the accountability of the data controller are met.[72]

De Hert and Gutwirth further distinguish between privacy and data protection based on their respective objectives, although they emphasise that the objectives align with the two concepts.[73] Nonetheless, they think such an equation would be a narrow conception. They argue that the main aim of data protection is to protect data subjects from unjustified data processing. This understanding, according to De Hert and Gutwirth, is on all fours with the right to privacy that seeks to safeguard against unjustified interferences in one's personal life. From this understanding, they argue that this might inform many scholars' attitude to consider data protection and privacy interchangeably.

De Hert[74] and Bygrave[75] appear to share a fundamental agreement, namely, that privacy undeniably holds a central role in data protection law, but labelling data protection law as solely or even primarily focused on safeguarding privacy is misleading.

Truly, in the case of *Bavarian Lager Co Ltd v Commission of the European Communities*[76] the Court noted that while the right to data protection might be a feature within the broader context of 'private life', as per the European Court of Human Rights, not all personal data inherently is measured 'private life'. This Court's line of thought may be grounded in the acknowledgment that certain facts about an individual, such as one's height, complexion and body build, inherently are part of public life simply by their existence.[77]

This article subscribes to the notion that privacy and data protection bear substantial yet distinct similarities. This stance is reached by recognising that issues related to data protection and privacy, to some extent, are practical considerations.[78] Essentially, the legal analysis of privacy and data protection must be conducted within the specific context in which they befall. Privacy is not a concept that can apply universally to different situations.[79] Solove's bottom-up approach involves conceptualisation of privacy by considering context-specific.

72 P de Hert & E Schreuders, *'The Relevance of Convention 108'* (2001) 33,42, Proceedings of the Council of Europe Conference on Data Protection, Warsaw, 19-20, November, 2001 cited in *'EU Study on the Legal Analysis of a Single Market for the Information Society'* (2009), Chapter 4, p.4.

73 P de Hert & S Gutwirth 'Data protection in the case law of Strasbourg and Luxemburg: constitutionalism in action' in S Gutwirth and others (eds) *Reinventing data protection* (2009) 3.

74 As above.

75 LA Bygrave 'The place of privacy in data protection law' (2001) 24 *University of New South Wales Law Journal* 282.

76 *The Bavarian Lager Company Ltd v Commissioner of the European Communities* ECR T-194/04, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62004A0194:EN:HTML (accessed 20 December 2021).

77 *Bavarian Lager Company* (n 76) 118.

78 Solove (n 51).

79 As above.

This means scrutinising privacy violations as disturbances of specific practices and regulations, such as interfering with peace of mind, intrusion on solitude, or loss of control over facts.[80] In examining the practices under the UBR, it is important to analyse whether in the context of the law, the UBR's practices offer a pragmatic response to data protection. Are there modern solutions for the potential problems created by the UBR?

7 Scope of data protection law in Malawi

7.1 Right to privacy under the Constitution as encompassing data protection

A discussion of enacted laws in Malawi arguably starts with reference to the Constitution of Malawi.[81] The rationale is that the Constitution is the supreme law.[82] Chapter IV of the Malawian Constitution contains provisions for human rights that must be respected and upheld by the branches of government. Additionally, these rights, where applicable, apply to all natural and legal persons in Malawi.[83] One of these rights is the right to privacy. Data protection can ensure that the right to privacy is safeguarded.

Section 21 of the Republican Constitution of Malawi provides for the right to personal privacy.[84] It provides as follows:

> Every person shall have the right to personal privacy, which shall include the right not to be subject to –
>
> (1) searches of his or her person, home or property;
> (2) the seizure of private possessions; or
> (3) interference with private communications, including mail and all forms of telecommunications.

In its enacted form, the section does not address the concerns of data protection. In this regard, it may be argued that there is a traditional conception of privacy under section 21 of the Malawian Constitution, which is not technology responsive.

Nyemba argues that section 21 of the Constitution is wide and may be interpreted to cover the right to privacy as also including the right of the individual to have their data protected.[85] This article agrees with the aforementioned observation. However, such wide interpretation would only

80 As above.
81 Republic of Malawi (Constitution) Act 20 of 1994.
82 As above.
83 Malawi Constitution (n 81) sec 15(1).
84 https://www.constituteproject.org/constitution/Malawi_2017#s166 (accessed 20 September 2023).
85 Nyemba (n 28).

be supported as a result of judicial pragmatism owing to the absence of a clear provision in the Constitution on the need to protect personal data. Regardless, by providing for the right to privacy, the article argues that section 21 of the Constitution encompasses data protection as the obligation therefore extends to data processors not to interfere with the privacy of individuals, owing to this constitutional right.

The right to privacy as it appears under the Malawian Constitution is coined in almost similar fashion with the provisions in article 12 of the Universal Declaration,[86] which proscribes arbitrary interference with a person's privacy and accords persons protection before the law against such interference. The Universal Declaration is enforceable as part of municipal law in Malawi.[87] The only differentiating feature with section 21 of the Malawian Constitution is that article 12 of the Universal Declaration appears to be narrow and limited.[88]

In December 2013 the United Nations General Assembly Resolution on the right to privacy in the digital age approved the General Comment of the United Nations Human Rights Committee on the right of privacy, family, home, correspondence, and protection of honour and reputation under ICCPR.[89] The General Comment calls for concise laws to protect the right to privacy, especially in the case of state surveillance and data processes.[90] To uphold the right to privacy, state parties must have precise laws in their surveillance activities, including the social protection sector such as the UBR. It is essential to ensure that individuals' privacy is protected, and clear laws can help achieve this.

General Comment 16 on the right to privacy, family, home and correspondence, and protection of honour and reputation (on article 17) of 1988, and General Comment 19 on the insurance of the family, the right to marriage and equality of spouses (on article 23) of 1990 hold significant importance in the realm of data protection.[91] These observations aim to address the gaps that emerged with the initiation of data protection discourse in the right to privacy sphere. They are crucial because they provide guidance on safeguarding personal data while protecting an individual's right to privacy. By emphasising the importance of protecting family, home, and correspondence, these General Comments highlight the need for privacy in all aspects of life, including the digital world.

86 Universal Declaration of Human Rights (Universal Declaration) adopted 10 December 1948.
87 The Universal Declaration is enforceable in the courts of Malawi as per *R v Chihana* (MSCA Criminal Appeal 9 of 1992) [1993] MWSC 1 (28 March 1993) where it was held that '[w]e accept that the UNO Universal Declaration of Human Rights is part of the law of Malawi and that the freedoms which that Declaration guarantees must be respected and can be enforced in these Courts'.
88 The same applies to art 17 of ICCPR.
89 Malawi is a state party to ICCPR having ratified it on 22 December 1993.
90 https://privacy.sflc.in/universal/ (accessed 3 January 2022).
91 C Kuner, *An International Legal Framework for Data Protection: Issues and Prospects', Computer Law & Security Review,* (2009), *Vol. 25, No.4, pp.307-317, at p. 308.*

General Comment 16 on article 17 of ICCPR acknowledges that the right to privacy is not only limited to its previous traditional conception. It is thought that General Comment 16 was passed because of the narrow framing of article 17 of ICCPR. Additionally, it may be argued that General Comment 16 augurs well with the principle of legal certainty which requires laws to be definite and clear. General Comment 16 is partly couched in the following terms:

> 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 authorised by law to receive, process and use it, and is never used for purposes incompatible with the Covenant. In order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to, ascertain which public authorities or private individuals or bodies control or may control their files. If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination.[92]

The effect of this General Comment is that the realm of data protection is placed under the wings of the right to privacy under ICCPR as well as the Universal Declaration. Section 211 of the Malawian Constitution provides for the legislative force of international law which Malawi.[93] It provides as follows:

(1) Any international agreement entered into after the commencement of this Constitution shall form part of the law of the Republic if so provided by an Act of Parliament.
(2) Binding international agreements entered into before the commencement of this Constitution shall continue to bind the Republic unless otherwise provided by an Act of Parliament.
(3) Customary international law, unless inconsistent with this Constitution or an Act of Parliament, shall form part of the law of the Republic.

Effectively, therefore, protection of personal data is provided for under the law in Malawi. The first reason is that Malawi has been a state party to ICCPR since 22 December 1993.[94] Since Malawi ratified ICCPR before the commencement of the Constitution, ICCPR is enforceable as part of domestic law.[95] The second reason is that section 11(2)(c) of the Constitution enjoins the courts to interpret the Malawian Constitution in line with international law norms, and that,

92 Human Rights Committee General Comment 16: Article 17 (Right to Privacy) The right to respect of privacy, family, home and correspondence, and protection of honour and reputation para 10.
93 https://www.constituteproject.org/constitution/Malawi_2017#s2234 (accessed 21 September 2023).
94 https://tbinternet.ohchr.org/_layouts/15/TreatyBodyExternal/Treaty.aspx?CountryID=104&Lang=EN (accessed 21 September 2023).
95 TT Hansen 'Implementation of international human rights standards through the national courts in Malawi' (2002) *Journal of African Law* 31.

therefore, the privacy provision under the Constitution may be interpreted in reference to General Comment 19.[96]

In this regard, it may be argued that based on section 21 of the Constitution and articles 12 and 17 of the Universal Declaration and ICCPR respectively, the requirement of data protection under the law subsists.

8 The Electronic Transactions and Cyber Security Act

The Electronic Transactions and Cyber Security Act 2016 (ETA 2016)[97] entered into force on 1 June 2017. It may be considered as the first major attempt to address data protection and privacy issues in Malawi. The long title to the ETA 2016 provides as follows:

> An Act to make provision for electronic transactions; for the establishment and functions of the Malawi Computer Emergency Response Team (MCERT); to make provision for criminalising offences related to computer systems and information communication technologies; and provide for investigation, collection and use of electronic evidence; and for matters connected therewith and incidental thereto.

As can be seen from the long title, the Act's objectives are diverse, as noted by Nyemba.[98] One of the objectives appears in Part VII which provides for data protection and privacy. Part VII is brief and is contained in four sections of the ETA 2016.[99]

Section 71 of the ETA 2016 outlines a data controller's responsibilities. A number of requirements are outlined in section 71(1) when handling personal data. Section 71(1)(a) stipulates that a data controller is obligated to guarantee that all data is processed lawfully and fairly. This is the first requirement. Second, section 71(a)(b) states that information must be gathered with specific, explicit and legal reasons in mind and cannot be processed in a manner that is inconsistent with those goals. Section 71(1)(c) establishes the minimal data dealing principle. Users of data must gather only information that is sufficient, pertinent, and not excessive in light of the reasons for which the data is being gathered and processed. Section 71(1)(d) lays down the fourth condition, which calls on data controllers to ensure that the data they collect is accurate and, if needed, kept up-to-date. Building on the necessity of maintaining accurate data, section 71(1)(e) mandates that data that is incomplete or wrong be erased or corrected in light of the reasons for which it was gathered or processed further. According to

96 Malawi Constitution secs 107 & 11(2) (c); R Kapindu J 'The relevance of international law in judicial decision-making in Malawi' Paper presented at the Judicial Colloquium on the Rights of Vulnerable Groups, held at Sunbird Nkopola Lodge, Mangochi, Malawi, 6 and 7 March 2014.

97 Cap 74:02 of the Laws of Malawi, 'Electronic Transactions and Cyber Security Act', https://malawilii.org/akn/mw/act/2016/33/eng@2017-12-31 (accessed 21 September 2023).

98 Nyemba (n 28).

99 ETA (n 97) secs 71-74.

section 71(1)(f), the data controller's last obligation is to retain data in a format that makes it possible to identify data subjects for as little time as is required for the purposes for which it was originally collected or for which it is subsequently processed. The right to be forgotten has anything to do with this. It mandates that data controllers retain information for as long as is required to fulfil the objectives for which it was gathered. One could argue that this criterion ensures that the hazards related to data storage are kept to a minimum.

The ETA 2016 allows for the processing of personal data in section 71(2). According to section 2 of the ETA 2016, processing of data includes any action or sequence of actions taken in relation to data, whether or not they are carried out automatically. These actions include gathering, logging, organising, storing, adapting or altering, retrieving, consulting, using, disclosing via transmission, disseminating, or otherwise making available, aligning or combining, blocking, erasing, or destroying data.

A need for data processing is provided by section 71(2)(a), which states that processing of data is permitted only with the consent of the data subject. In this context, consent refers to the requirement that the data subject be informed of the intended data processing's aims and, as a result, that the consent comes from their free will.[100] Data processing is made possible by section 71(2)(c), which essentially enables a data controller to carry out his legal obligations. One instance of this would be if the authority sought reports from a data controller regarding the processing of data.

Subject data may also be processed under section 71(2)(e) if the processing is done in the public interest or in accordance with an official authority. According to section 71(2)(f), processing of personal data is allowed if it serves the legitimate interests of the data controller, a third party, or parties to whom the data is disclosed. However, in cases where the data subject's fundamental rights and freedoms are more important than these legitimate interests, processing of the data is prohibited.

It is evident from the aforementioned clauses that there are several restrictions on data processing. On the other hand, one could counter that the data controller has broad authority over data processing. In light of the diverse definition of data processing provided in section 2 of the ETA 2016, this point has been made. It is opined that the definition section should have included the definitions of the various components of the definition. In its current state, the data controller may perform various acts related to personal data and still fall under lawful data processing. An example of this relates to collection. The ETA 2016 does not expound on the prerequisites to lawful collection. Elsewhere, consent as related

100 ETA (n 97) does not define consent but rather provides what constitutes consent. This understanding, it may be argued, is guided by art 1(2) of the SADC Model Law on Data Protection.

to consent relates to freely-given, unambiguous consent. It further empowers the data subject to withdraw consent after having given it. It also mandates that data controller to keep a record of the permission.[101]

The rights of data subjects are outlined in section 72 of the ETA 2016. It gives the data subject the free right of access to their personal records about themselves without any costs to them. To verify whether their data is being processed, the data subject has access to it. The data subject has the right of communication on the processing, sources, and possible recipients of the subject's data according to sections 72(1)(a) and (b). A data subject may object to data processing under section 72(2) for valid reasons. There is a claim that doing so guarantees the data subject a remedy. The second remedy is for the data subject to request the rectification, erasure, or blockage of any data whose processing violates this Act's rules, particularly if the data is incomplete or erroneous. This need is consistent with General Comment 16 on article 17 of ICCPR and the obligations placed on a data controller in sections 71(1)(d) and (e), as previously stated, which demand accurate data.

Section 73 of the ETA mandates the data controller to notify the data subject of the name of the data controller or his representative, the purposes for which the data is collected, and the data subject's rights in order to enable the data subject to give informed consent.

Section 74 of the ETA 2016 is particularly significant as it mandates the data controller to put in place organisational and technical safeguards to protect personal data from unauthorised access, disclosure, alteration, and destruction – including accidental loss, theft and alteration – as well as from all other unlawful forms of processing, especially when the processing involves the transmission of data over a network. Therefore, section 74 protects data subjects' privacy by means of safeguards established by the controller, including protocols and other standard working documents.

9 Access to Information Act

Section 20 of the Access to Information Act (ATI) is of special relevance. It states that information concerning a third party must not be shared until it has been determined whether the information indeed is secret and whether disclosure would be damaging. Section 29 further states that personal information must not be provided in an unreasonable manner. It might be claimed that leaving the determination of when to share data or not to the information holder exposes the entire provision to misuse. Consent must be a fundamental tenet. Furthermore, it

101 General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (GDPR).

is suggested that the acts be linked with references to each other for consistency's sake. The other alternative route is to have a consolidated piece of legislation.

10 Informative international instruments and aspirations on data protection

10.1 General Data Protection Regulation

The General Data Protection Regulation (GDPR) is the data protection regulation of the European Union (EU). GDPR entered into force in 2016. By 25 May 2018 all organisations were mandated to be GDPR compliant. GDPR is applicable to member states of the EU. A salient feature of GDPR is that it also has extraterritorial application in that data processors may fall under the purview of GDPR so long as the data subjects that are targeted and/or the data that is collected relates to people in the EU.

Of particular interest in GDPR is article 5. It guides principles that should guide personal data processing. There is a total of seven principles. The first is the principle of lawfulness, fairness and transparency. It entails the need to process data in circumstances that are permitted by law, based on fair considerations and in a manner that is sufficiently transparent. The transparency, it may be argued, should involve the data subject as the centre piece of data processing. It could also involve putting in place mechanisms that safeguard the right of access and information to the data processing by the data subject where possible.

The second is purpose limitation. This principle requires that data is collected for specified, clear and valid purposes. Consequentially, therefore, data must not be processed for any other means that are incompatible with the purposes for which it was initially collected. Nonetheless, there is a caveat in that data collected for other purposes may be further processed where the public interest so demands, or where research purposes for historical, scientific or statistical ends may so require. This, in line with article 89(1), is not to be considered incompatible with specified purposes for which the data was initially collected.

The third principle under article 5 of GDPR is data minimisation. This principle is brief. It requires that data should be only sufficient for the purposes for which it is collected, relevant and limited to those purposes, as much as necessary.

The fourth principle is accuracy. Data should be accurate in relation to the 'actual' data subject and that, where necessary, data processors must put in place mechanisms that ensure that the data is up-to-date. Any inaccuracies must be rectified or erased without delay.

Storage restriction is the fifth principle. In accordance with the purpose restriction principle, this concept mandates that data storage that identifies the data subject be kept for no longer than the period of the reasons for which it was obtained. The exception is processing for archiving purposes which, as stated in article 89(1), does not contradict the reasons for which data is gathered. As a result, the same may apply to the length, as long as the archiving is for the objectives specified in the discussion of purpose restriction. This exception, however, is subject to the execution of the relevant technological and organisational measures required by the rule to protect data subjects' rights and freedoms.

The final but one principle is the integrity and secrecy principle. The essence of this concept is the requirement to safeguard personal data through suitable technological and organisational safeguards. Among other things, the procedures should strive to avoid illegal data processing, inadvertent data loss, and unauthorised access.

The final element is accountability, which requires the data controller to be accountable and demonstrate compliance with the six criteria listed above.

GDPR is also praiseworthy for granting data subjects additional rights. These include the right to information; access; rectification; erasure; restriction of processing; data portability; and objection to processing. This article will not go into further depth on these rights as it is slightly outside the scope of the article.

10.2 African Union Convention on Cyber Security and Personal Data Protection

The African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) was accepted on 27 June 2014 during the AU Assembly's twenty-third ordinary session in Malabo, Equatorial Guinea. It currently has only been signed by 16 nations, approved by 13 countries, and lodged by 13 countries.[102] Malawi is not a state party to the Convention. Problems of non-domestication are not alien. Various reasons, such as the domestication process, have been proffered. For example, the AU Report on Malawi's non-compliance with its protocols and charters notes as follows:

> The limited domestication of international protocols, including those of the African Union, is considered to be largely a result of [Malawi's]domestication system. While the exclusion of Parliament from the ratification process ensures a relatively speedy process of ratification, the main drawback is that in the long run, law-makers (Members of Parliament) are less aware of the instruments that the country is a

102 https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection (accessed 4 January 2022).

signatory to or not. As a result, the National Assembly is not in a position to make reference to them when debating legislation.[103]

Malawi's non-ratification of the Malabo Convention may only be speculated upon, but the reasons noted in the above report may be relevant.[104]

Article 11 of the Malabo Convention requires governments to establish a self-governing administrative entity entrusted with protecting personal data. Article 12 of the Convention requires nations to impose restrictions on the processing of personal data, including restrictions based on public interest and storage. One of the primary shortcomings of the Convention is that it does not define lawful data processing. Ball has also identified this as a significant component of the Convention that may expose data processing to the data controller's subjectivity.[105]

One of the Malabo Convention's significant innovations is the notion of consent. According to article 1 of the Convention, consent is the expression of a definite, explicit and informed will with regard to the data that a data processor requests to handle. The permission might come from the data subject themselves or from their legal, judicial or treaty representative.

10.3 The SADC Model Law on Data Protection

2013 saw the adoption of the SADC Model Law on Data Protection, which was created in 2010. The goal of the member nations is to protect personal information. The goal of this regional endeavour is to guarantee data privacy for all member states in the area. Similar to the Malabo Convention, the Model Law's definition of consent is one of its most notable features. Consent is defined under the SADC Model Law in the same way as the Malabo Convention.[106] The central piece of this definition is the need for clear consent on the part of the data subject. Part III of the Model Law also provides for a data protection authority tasked with regulatory powers for data protection. This is a good innovation as it provides for a specialised authority to carry out supervisory powers to ensure data protection.

Under the SADC Model Law, the processing of personal data is subject to the same requirements as under GDPR. Thus, it can be observed that the Model Law only followed the EU legal framework's data processing methodology. On the other hand, the SADC Model Law deserves praise for focusing specifically on the handling of private information. It forbids the processing of sensitive personal

103 'Malawi's compliance with African Union charters and protocols' State of the Union, AU, 2015.
104 As above.
105 K Ball 'Introductory note to the African Union Convention on Cyber Security and Personal Data Protection' *International Legal Materials* 1, <DOI: https://doi.org/10.1017/ilm.2016.3 (accessed 20 February 2022).
106 SADC Model Law on Data Protection art 1(2).

data that might expose the identities of the data subjects, thereby putting them at greater risk.[107] However, if a data subject provides consent, the data may be processed in accordance with the legal provisions that allow for such consent to be granted.[108]

The ETA 2016 and the data controller's responsibilities are nearly identical, with the latter requiring the former to inform the former about the processing of the subject's personal data.

Organisations must also include organisational and technical safeguards against unintentional access, careless erasure, destruction or alteration, according to the SADC Model Law.[109] The SADC Model Law's article 31 gives data subjects rights regarding data controllers. In essence, the person whose data is being processed has control over the actions taken with respect to that data. In summary, the SADC Model Law indicates a strong regional aim for the protection of personal data and presents a complete strategy.

The major drawback of the Model Law is on the remedies and rights of data subjects. Literacy levels may militate against the illiterate accessing remedies that require written notices. Additionally, the Model Law does not make provision for decentralisation or mobile operations of the data authority to ensure that even the poor are reached and have access to remedies under the law.

11 Personal data protection under the Universal Beneficiary Registry

11.1 Protection of personal data under the UBR

A number of the UBR Protocols' clauses are designed to protect personal information. The requirement for consent before processing data is the main one. Section 71(2)(a) of the Electronic Transactions and Cyber Security Act is in compliance with this requirement. The UBR Protocols provide a number of noteworthy data protection features. For example, they mandate all personnel – employees, contractors, consultants and visitors – to acquire knowledge of the information security policies, guidelines, processes and mechanisms, and they also have a responsibility to secure the UBR's information assets. Additionally, accessing or using UBR assets without permission from the UBR management team is prohibited by the UBR Protocols.

107 SADC Model Law on Data Protection Part V, art 15.
108 As above.
109 SADC Model Law on Data Protection art 24.

It is necessary to notify the UBR administrator of security breaches that could expose data to unauthorised dissemination. The rules specify that a failure to familiarise oneself with the UBR's security standards will not be accepted as an excuse, presumably in an effort to ensure that all staff members handling UBR data understand them.

It is necessary to notify the UBR administrator of security breaches that could expose data to unauthorised dissemination. The rules specify that the failure to familiarise oneself with the UBR's security standards will not be accepted as an excuse, presumably in an effort to ensure that all staff members handling UBR data understand them.

Furthermore, handling data on personal and portable devices is forbidden by the UBR Protocols. It is believed that this lowers the possibility of loss that accompanies the carrying around of portable electronics. Furthermore, data users must set up safeguards to protect the confidentiality and integrity of personal data in accordance with UBR Protocol Section 3.1.1(h). One could argue that this obligation imposes a fiduciary duty on data users to behave in the subjects' best interests. The Protocols demand special vigilance when handling printed extracts of shared UBR data as data may also be stored in hard copy format.

The above requirements agree with the provisions of section 74 of the ETA which provides as follows:

> (1) A data controller shall implement technical and organisational measures enabling to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.
> (2) Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

Five primary security goals are identified by the UBR under Part 4 of the UBR Protocols. 'Security obligations' appear in the marginal notes of section 74 of the ETA. The UBR's security objectives are intended to help it fulfil its security-related responsibilities. The UBR's primary security goal is 'availability'. It implies that there must be enough security measures in place to guarantee recoverability in the case of an interruption and that the personal data stored there is accessible to authorised users, clients and business partners when needed.

The second security objective is 'integrity and competence'. This objective aims at ensuring that the information held by the UBR is accurate and complete as far as necessary during the entire information processing cycle. This objective arguably stems from section 74 of the ETA above but is also in agreement with section 71(1)(e) of the ETA which requires accuracy of data.

'Confidentiality' is the third security goal under the UBR Protocols, and it calls for sufficient safeguards or controls to guarantee that information is only given to or made available to authorised processes, entities or individuals. The Constitution's section 21 guarantees the right to privacy. When those providing data do so, they do so solely to fulfil the objectives of the data collection. Therefore, it is important that such data be kept private and used only for those purposes after it has been gathered.

The fourth security objective under the UBR Protocols is 'authenticity', which requires adequate controls or safeguards to be in place to uniquely identify users of information assets to the information being accessed. This security objective is in line with section 74 of the ETA, which charges data controllers to put in place technical and organisational measures to safeguard data. In this regard, the security objective charges data users of the UBR framework with responsibility for the information which they access. In other words, the UBR management team seeks to achieve certainty that the partners they are dealing with are legitimate players in the social support strengthening programmes who may be held accountable for their actions.

The last security objective under the UBR Protocols is 'accountability'. It enjoins data controllers to be responsible for the data that they process, and to be accountable for their actions. This further means that the data controllers must adopt deliberate safeguards to ensure that any single controller is responsible for the data they process and their actions in relation to the same. Data controllers and users exercise their functions on the basis of trust. It is only pertinent that they should be held accountable for their actions.

11.2 Adequacy of data protection under the UBR

To a larger extent than not, the UBR Protocols have attempted to offer data protection. However, as was already mentioned, privacy primarily is the responsibility of the data subject, who aims to limit the amount of personal information that may be made public. Nevertheless, an examination of the UBR Protocols has shown that the topic of the data is only mentioned in passing. The 29-paged Protocols contain two instances of the term 'data subject'. It is crucial that the information that data processors have about a data subject is centred around them.

The ETA's section 73 grants the data subjects a number of legal rights. The first of these is the right to know the identity of the data controller and the reasons behind the collection of personal data. The right to object is the last and, possibly, most important right of the data subject. For valid reasons, one may object to the processing of personal data. The information processing may cease to involve a particular data subject in the event that the data subject raises an objection. The requirement that any such objection be supported by a valid

argument is a restriction, nevertheless. Finally, a data subject has the right to request, from a data controller, the correction, erasure or blockage of data of which the processing violates the Act's requirements, particularly where the data is erroneous or incomplete.

Although certain rights fall within the recently-described requirements, they do not grant the data subject a direct right of action against the data controller, which includes the UBR, data users and/or third parties. In this context, one could contend that the rights granted to the data subject by the ETA are of a remedial character. According to the opinion, if the same had been ingrained in the procedures, they would have been procedural and would have given a data subject greater certainty regarding the protection of their privacy.

Additionally, the UBR Protocols are contractual in nature. In general, they cover the agreement between data users and data controllers. By their legal nature contractual arrangements are between the parties to such an arrangement. It is trite, therefore, that rights and obligations under such arrangements are a matter of principle between the parties. The sobering thought is the recourse that a data subject has against a third party that might have illegally accessed their personal information. This would occur even where the data user has undertaken all contractually-necessary steps.

Under part 8 of the UBR Protocols, to protect the privacy of data, the only provision dealing with third parties cautions against data sharing with third parties. It declares that if data is shared with unaffiliated parties, the data user will be held accountable and subject to legal consequences. As much as is it realistic that data may be exposed to third parties, this poses a potential challenge for a violation of rights of data subjects. However, there are remedies in the law as observed in the UBR Protocols, such as section 84 of the ETA which deals with unauthorised data access by third parties.

12 Concluding remarks: Personal data protection in Malawi

The Electronic Transactions and Cyber Security Act represented Malawi's most significant attempt to address data protection issues.[110] The Act is both a civil and penal legislation. The ETA defines personal data as any information about an individual that could be used to directly or indirectly identify that specific individual via the use of different aspects.[111] Section 3 of the ETA provides for the objectives of the Act. Section 3(a)(ii) provides that one of the objectives is to balance societal and individual interests in the exploitation of information. Section 3(c) provides a further objective, which is to ensure that there exist proper mechanisms to ensure data protection, among others. Section 3 of the

110 ETA (n 97).
111 ETA (n 97) sec 2.

ETA makes it clear that the Act's responsibility is to safeguard data subjects' personal information.

The Malawi Communications Regulatory Authority is tasked with implementing the ETA in accordance with section 5. The Act, however, is silent about a data protection authority. The Act does not provide for the appointment of a data protection authority, in contrast to other sections, such as section 6, that establishes the Malawi CERT, and section 75 that appoints the domain registrar in charge of managing the .mw domain.

The statute appoints a data protection authority to manage data protection issues, following international legislative practice. Part III of the SADC Model Law on Data Protection, for example, establishes a data protection authority. According to the SADC Model Law, one of the persons tasked with ensuring that the controller's data processing conforms with the law is the authority.[112] As mandated by the SADC Model Law, the authority is also responsible for creating subsidiary laws in the form of rules that are enforceable statutory instruments.[113] Other provisions under article 4 of the SADC Model Law entitle the authority to make enquiries of its own accord or after having received complaints, into data protection issues. The authority under the SADC Model Law is also to be empowered to receive complaints by various means.

This is where the Electronic Transactions and Cyber Security Act's legislative approach falls short. According to this research, it would resemble carrying water in a leaky bucket to lay out the obligations of data controllers and the rights of data subjects without a framework to enforce them. The Act makes no mention of any protective authority's responsibilities.

Nonetheless, the Malawi Communications Regulatory Authority, as earlier presented, is tasked with implementing the ETA. In this regard, the MACRA Board may simply establish a directorate of data protection. However, this may be undesirable and with less effect as the directorate is not directly provided for under the Act. Therefore, it is believed that the appropriate course of action in this case may be to create specific provisions under part VII of the ETA that explicitly grant MACRA – referred to as the authority under section 2 of the ETA – the right to adopt the SADC Model Law's framing and give it the explicit authority to create regulations for the protected privacy and data. Alternatively, as in other statutes, the Act may specify the authority's functions.[114] The advantage of this is that it achieves one of the law's desirable qualities, which is certainty.

112 ETA (n 97) art 4(1)(a).
113 ETA (n 97) art (1)(d).
114 Eg, Cap 48:09 of the Laws of Malawi, 'Competition and Fair Trading Act,' clearly spells out the functions of the Competition and Fair Trading Commission under sec 8.

Establishing data protection authorities is a requirement of the African Union Convention on Cyber Security and Protection of Personal Data for state parties.[115] In contrast to the SADC Model Law, the AU Convention stipulates that the data protection authority must be an independent body.[116] Given that MACRA also performs other legal duties unrelated to data protection, it would be considered inappropriate for data protection purposes in this regard.

However, it is opined that having MACRA to be the authority would assist Malawi in saving resources. This is because new staff recruited would share infrastructure and other economic resources with an already-established system. Establishing an independent authority would mean an extra board for the government. This research is of the view that the legislative approach under the ETA with regard to the authority responsible for data protection fits our economic realities. On the other hand, the benefits of an independent authority are that there would be a concentration of expertise, unlike if data protection were regulated by a non-specialist authority whose board is diversely drawn.

The government should consider ratifying the AU Convention on Cyber Security and Personal Data Protection, as its provisions for a data protection authority are precise and appear to align with Malawi's social, cultural and economic conditions.

12.1 The Draft Data Protection Bill

Malawi's intentions and goals for a data protection framework are reflected in the Draft Data Protection Bill. For the purpose of comparative legal analysis, the Data Protection Bill is discussed. One of the objectives of the research was to conduct a comparative law analysis. It is only pertinent that the legislative aspirations are measured against comparable law to better understand whether the approach taken has the potential of safeguarding personal data under schemes such as the UBR.

The 2021 Draft Data Protection Bill's lengthy title states that it is an Act to make provision for protection of personal data, for regulation of the processing of personal data, and for matters connected therewith or incidental thereto.

The Malawi Communications Regulatory Authority will continue to be the body responsible for safeguarding personal data, which is the first noteworthy aspect of the Data Protection Bill. The Draft Data Protection Bill's intentions are explicit, in contrast to those of the ETA. For example, section 3's goals include ensuring that processing personal data conforms with data protection standards,

115 African Union Convention on Cyber Security and Protection of Personal Data art 11.
116 African Union Convention on Cyber Security and Personal Data Protection (n 88)

such as privacy and data security.[117] Additionally, the Bill aims to protect data subjects' rights regarding the handling of their personal information.[118] The fact that the Bill also aims to control cross-border transfer of personal data is one of the noteworthy introductions to the discussion of data processing in Malawi. The law did not specifically provide for the protection of personal data with relation to cross-border transmission under the former system, primarily part IV of the ETA.

Section 5 of the Draft Data Protection Bill is noteworthy as it provides an exemption from processing personal data obtained for home, recreational or personal purposes. Given that the data subject's rights are still at risk, the research has not been able to understand the justification for such an exemption. For example, it would be problematic if a leisure club that gathers member data was discovered to have violated the Act and then allowed to continue operating without consequences.

Additionally, the Draft Data Protection Bill keeps MACRA as the body in charge of putting it into effect.[119] In section 8 it states that MACRA, the authority, would have a data protection unit. Thus, the section 5.2 explanation of the data protection authority's independence is applicable here, *mutatis mutandis*. According to the research, an independent data protection authority is recommended for the previously-mentioned reasons.

The principles for data processing are provided for in section 18 of the Draft Data Protection Bill. The ETA, the SADC Model Law and the AU Convention on Cyber Security and Data Protection are all reflected in the guiding principles. Based on the research, it is concluded that the data processing principles should be adhered to in terms of methodology. The principles protect data subjects' rights in accordance with section 21 of the Constitution, which protects data subjects' privacy through the right to privacy. However, these principles are the same as those provided for under section 71(2) of the ETA. It therefore does not make much legislative sense to have provisions in two Acts of Parliament that mirror each other. It is opined that the provisions in the ETA regarding data processing should, therefore, be repealed once the Data Protection Bill enters into force.

The issue of data protection pertaining to children is also included in the Draft Data Protection Bill. It stipulates that a legal guardian's consent is required.[120] This is a welcome approach as the previous regime did not address the issue of data privacy for minors.

117 Draft Data Protection Bill sec 3(a), https://digmap.pppc.mw/wp-content/uploads/2022/03/Malawi-Data-Protection-Bill-final-draft-210630-.pdf (accessed 22 September 2023).
118 Draft Data Protection Bill (n 117).
119 Draft Data Protection Bill (n 117) sec 6.
120 Draft Data Protection Bill sec 20.

It is believed that if the Bill is approved by the legislature, the legal protection of personal information will be enhanced. As a result, programmes such as the UBR that protect personal data will be protected.

13 Implications of Malawi's Current regulatory framework on the UBR data-sharing framework and personal data protection

Administrative remedies for breaches of personal data are not provided by the Protocols, as was mentioned during the UBR's examination of the data protection framework. For this reason, section 35 of the Draft Data Protection Bill is relevant. It offers guidelines by which a data controller can be considered to provide sufficient data protection. A few of these are the existence of legally-binding rights for data subjects, their capacity to seek judicial or administrative recourse to protect their rights, and the rule of law in general.[121]

It was noted that data sharing under the UBR is contractual in nature. One of the challenges noted with this arrangement was the security objective of authenticity of the data user. However, since section 37 of the Draft Data Protection Bill mandates data users' registration, this issue might be resolved.

The following are some ways in which the current legislative framework affects the UBR and personal data protection: The Constitution and part VII of the ETA do not fully guarantee the right to data protection. Since the SADC Model Law on Data Protection and other instructive international documents are in line with regional ambitions, it is vital that the UBR data sharing framework implement procedures for the protection of personal data at all times. Respecting section 71 of the ETA's data processing guidelines is another aspect in this regard. Section 74 of the ETA requires the UBR data-sharing framework to establish adequate organisational and technical safeguards for the security and protection of personal data. However, in situations where there has been a breach of a data subject's personal information, the existing legal system does not offer the data subject primary remedies. It is argued that this could have a detrimental effect on the safeguarding of personal data because the legal system's redress procedures could be expensive and time-consuming.

The significance of a person's right to privacy has been highlighted in the article. Its primary focus was on the risks associated with the information society's gathering of personal data. Among the numerous risks are security lapses, illegal access, loss and erasure. The goal of the study was to establish how Malawian legislation protects the protection of personal data. It was discovered that Malawi has laws designed to protect personal information. The Electronic

121 Draft Data Protection Bill sec 35(2)(a).

Transactions and Cyber Security Act is one of the most notable of these. Ultimately, nevertheless, it was determined that the statute lacked the necessary comprehensiveness. Comparable laws, such as the AU Convention on Cyber Security and Data Protection, the General Data Protection Regulation and the SADC Model Law on Data Security, provided lessons throughout the research. As a result, it was suggested that the law should move closer to enacting an extensive data protection framework.

The study then looked into Malawi's actual practices for protecting personal data. A case study utilising the Unified Beneficiary Registry was conducted. According to the study's findings, the UBR had implemented organisational and technical safeguards to protect data subjects' personal information. Nonetheless, it was discovered that the UBR Protocols' most significant flaw was their failure to provide for data subjects' administrative rights. However, it was determined that the UBR provides reasonable safety for personal data.

The article's emphasis was redirected to data protection legislation processes, specifically focusing on the Draft Data Protection Bill. The investigation came to the conclusion that the UBR data-processing procedures are affected in a number of ways by the Draft Data Protection Bill. The requirement that data users register with the authority is one of these. The Draft Bill also mandates the use of administrative measures to protect the rights of data subjects.

The study further is of the view that the data protection authority in Malawi should be an independent body responsible for enforcing data protection laws.

In essence, the study's conclusion about Malawi's legislative procedures is that the country should take a comparative approach rather than attempting a wholesome adoption of regional and international data protection laws.