

**DATA PROTECTION WITHIN THE CLOUD:  
LESSONS FOR THE NEW AFRICAN DATA  
PROTECTION REGIME FROM THE EUROPEAN  
DATA PROTECTION FRAMEWORK.**

**OSCAR KOOME MBABU**

**DISSERTATION SUBMITTED IN PARTIAL  
FULFILLMENT OF THE BACHELOR OF LAWS  
DEGREE**

**MARCH 2016**



**Strathmore University**

**Law School**

**DATA PROTECTION WITHIN THE CLOUD: LESSONS FOR THE NEW AFRICAN  
DATA PROTECTION REGIME FROM THE EUROPEAN DATA PROTECTION  
FRAMEWORK.**

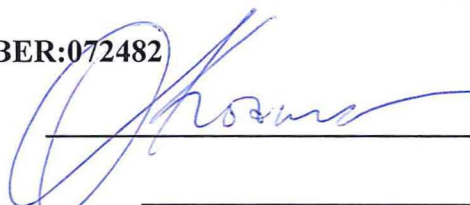
**DISSERTATION SUBMITTED IN PARTIAL FULFILLMENT OF THE BACHELOR  
OF LAWS DEGREE**

**STUDENT'S NAME:**

**OSCAR KOOME MBABU**

**STUDENT'S REGISTRATION NUMBER:072482**

**SIGNATURE OF STUDENT:**

  
\_\_\_\_\_

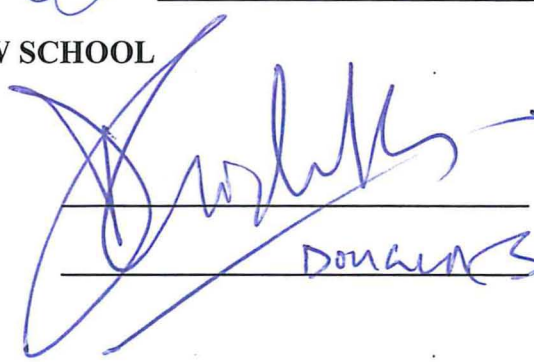
**DATE:**

\_\_\_\_\_

**STRATHMORE UNIVERSITY LAW SCHOOL**

**NAME OF SUPERVISOR:**

**SIGNATURE OF SUPERVISOR:**

  
\_\_\_\_\_  
**DOUGLAS GITHUKU**



**Strathmore University**

Law School



**Strathmore University**

**Law School**

**DECLARATION OF ORIGINALITY:**

I declare herewith, that this above-mentioned dissertation is my own original work. Furthermore, I confirm that: this work has been composed by me without assistance; I have clearly referenced in accordance with departmental requirements, in both the text and the bibliography or references, all sources (either from a printed source, internet or any other source) used in the work; – all data and findings in the work have not been falsified or embellished; this work has not been previously, or concurrently, used either for other courses or within other exam processes as an exam work; and that this work has not been published.

**SIGNATURE OF STUDENT:**



**Strathmore University**

**Law School**

**ACKNOWLEDGEMENT:**

I would like to appreciate the effort and sacrifice shown by my dear mother, Ms. Jane Kathure Ikunyua-Mbabu, whose diligence and undying love has strengthened me during the most tumultuous times of my academic life, and Mr. Lawrence Murithi Mbabu, my father, who has taught me the invaluable lesson that knowledge is power. Finally, I would like to acknowledge my younger brother, Dennis Muriungi Mbabu, I hope he strives to achieve greatness, twice as hard as his brother has.



**List of abbreviations:**

1. A29WP: Article 29 Working Party
2. AU: African Union.
3. DPD: Data Protection Directive
4. EU: European Union
5. FSA: Financial Services Authority.
6. IaaS: Infrastructure as a Service
7. PaaS: Platform as a Service
8. PNC : Police National Computer
9. SaaS: Software as a Service
10. WP136: Data Protection Working Party 136



**List of cases:**

**A. European Court Cases:**

1. *Bodil Lindqvist*, Case 101/01, [2004] QB 1014
2. *Campbell v Mirror Group Newspapers* [2004] UKHL 22 on appeal from [2002] EWCA Civ 1373 and [2002] EWHC 499 (QB).
3. *Douglas v Hello* [2007] UKHL 21 on appeal from [2005] EWCA Civ 106 and [2005] EWCA Civ 595, [2005] EWCA Civ 861.
4. *Österreichischer Rundfunk* Joined Cases C-465/00, C-138/01, and C-139/01 [2003] ECR I-4989.
5. *Durant v Financial Services Authority* [2003] EWCA Civ 1746.
6. *Scottish Information Commissioner v Common Services Agency* [2008] UKHL 47.
7. *Common Services Agency v Scottish Information Commissioner* [2008] UKHL 47.
8. *Volker und Markus Schecke (Approximation of laws)* OJ C 13/6. Joined Cases C-92/09 and C-93/09.
9. *Innovations (Mail Order) v Data Protection Registrar*, Case DA/92, available from <http://www.informationtribunal.gov.uk/DBFiles/Decision/i163/innovations.pdf>
10. *Johnson v Medical Defence Union*. [2007] EWCA Civ 262.
11. *CCN Systems v Data Protection Registrar*, [2006] EWHC 321 (Ch) Available from [http://www.informationtribunal.gov.uk/Documents/decisions/cnn\\_systems.pdf](http://www.informationtribunal.gov.uk/Documents/decisions/cnn_systems.pdf)
12. *Linguaphone Institute v Data Protection Registrar*, Case DA/94 31/49/1
13. *The Chief Constables of West Yorkshire, South Yorkshire and North Wales Police and the Information Commissioner* Available from [http://www.informationtribunal.gov.uk/DBFiles/Decision/i204/north\\_wales\\_police.pdf](http://www.informationtribunal.gov.uk/DBFiles/Decision/i204/north_wales_police.pdf)
14. *Chief Constable of Humberside Police and others v Information Commissioner*, [2009] EWCA Civ 1079.



**B. Kenyan Court Cases:**

1. *Benard Murage v. Fineserve Africa Limited and Four Others* (Petition No. 503 of 2014)
2. *Kipkalya Kones v Republic & Another exparte Kimani Wanyoike & 4 Others* (2008) 3 KLR (EP) 291,
3. *Francis Gitau Parsimei & 2 Others v National Alliance Party & 4 Others* (Petition No.356 and 359 of 2012)
4. *Speaker of National Assembly v Njenga Karume* [2008] 1 KLR 425,
5. *Damian Belfonte v The Attorney General of Trinidad and Tobago* C.A 84 of 2004,
6. *Harrkinson v Attorney General of Trinidad and Tobago* [1980] AC 265.
7. *Wananchi Group (Kenya) Ltd v The Communications Commission of Kenya* (Petition No.98 of 2012)
8. *Isaac Ngugi v Nairobi Hospital and Another* (Petition No.461 of 2012)
9. *Kennedy vs Ireland* (1987) I.R 587
10. *Republic v The Council of Legal Education ex parte James Njuguna and 14 Others*, Misc. Civil Case No. 137 of 2004 (unreported).





**ABSTRACT:**

The digital wave has finally hit Africa, and its effect upon the African economy has been immensely positive. With the development of innovative products such as Safaricom's M-Pesa money transfer service, as well as iCow, a farming digital product that has optimized dairy farmers' productivity, the consumer market has developed an appetite for sound, data-centric solutions in order to enhance the various socio-economic activities present within the Continent.

At the centre of the immense adoption of emergent technologies by the African populace is one of the most valuable resources present in the current technology era; data. The latter enables the adoption and execution of innovative strategies by multinational companies in order to minimise costs and maximise profits. Moreover, the widespread use of Big Data technologies and the incorporation of data into corporate strategies enables efficient market segmentation as solutions are tailor-made to suit specified clientele according to their needs. The latter leads to products that effectively lead to technological leaps and contribute immensely in terms of trickle-down benefits to the larger society. This could go a long way in combating familiar foes of African development such as ignorance (through educational platforms, such as Coursera), disease (through healthcare solutions such as HelloDoctor) and poverty (the kuhustle.co.ke application has enabled the provision of on-demand software services to the public through a bidding process, leading to access of cheaper affordable services for customers, while generating revenue for the biddee).

Despite the monumental opportunities presented by the advent of emergent technologies, specifically cloud technologies whose proliferation in Africa is abundant, the African Union's member states remain largely unprepared for the data presence within their jurisdictions. Only seven out of fifty-four African States have a working data protection policy, while the mobile phone industry continues to post sales of upto 50million units per year within the African market. The exposure to the violation of consumer rights as well as privacy rights guaranteed by the Universal Declaration of Human Rights is immense for citizens of African States.

This paper intends to analyse the various data protection principles sourced from the European Union, whilst juxtaposing it with the present African data protection regime, insofar as the recent adoption of the African Union's Convention on Cybercrime and Personal Data Regulation is concerned. This paper will also critically analyse the encounter between an emergent, cloud-based technology and the Kenyan jurisdiction, in the case of *Bernard Murage v. Fineserve Kenya Limited & Three Others*, in order to understand the state of Kenya's data protection standing in the current crisis. Finally, this paper will give the author's humble recommendations based on the view of more prominent Internet jurists who have dealt with the subject matter.



**Strathmore University**

Law School



Table of Contents

**CHAPTER ONE: RESEARCH PROPOSAL..... 1**

**Introduction:..... 1**

**JUSTIFICATION OF THE STUDY:..... 2**

**STATEMENT OF THE PROBLEM:..... 5**

**STATEMENT OF THE OBJECTIVES:..... 6**

**AN INTRODUCTION TO DATA PROTECTION: THE CONCEPT OF PROCESSING AND DATA PROTECTION ACTORS:..... 6**

        1. The concept of processing:..... 6

        2. Data Protection Actors: ..... 9

**Chapter Breakdown:..... 12**

        1. Chapter One: Research Proposal..... 12

        2. Chapter Two: Fundamental concepts and theories regarding Cloud Computing and the Emergence of data protection policy in the global digital market:..... 12

        4. Chapter Four: Analysing The Present Data Protection Framework Within The Kenyan Jurisdiction Through The Constitution, Kenyan Jurisprudence And The African Union Convention On Personal Data Protection And Cybersecurity: ..... 13

        5. Chapter Five: Conclusions and Recommendations: ..... 13

**CHAPTER TWO: FUNDAMENTAL CONCEPTS AND THEORIES REGARDING CLOUD COMPUTING AND THE HISTORY OF THE EMERGENCE OF DATA PROTECTION POLICY IN THE GLOBAL DIGITAL MARKET:..... 14**

**A. Cloud Computing:..... 14**

        1. Introduction:..... 14

        2. The Cloud Supply Chain: Key Concepts: ..... 16

**The Emergence of Data Protection in Contemporary History: ..... 23**

**CHAPTER THREE: DATA PROTECTION PRINCIPLES DERIVED FROM THE EUROPEAN UNION AND THEIR APPLICATION ON CLOUD-BASED TECHNOLOGIES: ..... 38**

    1. Personal data..... 38

    2. Sensitive data ..... 40

**2. Fair and Lawful Processing:..... 55**

        I. Fair Processing: ..... 55

        II. Lawful Processing: ..... 63



3. Unlawful acquisition of personal data:.....	67
4. The principles of adequacy and relevance:.....	69
5. Accuracy and Timeousness: .....	73
6. Data Security: .....	73
<b>CHAPTER FOUR: ANALYSING THE PRESENT DATA PROTECTION FRAMEWORK WITHIN THE KENYAN JURISDICTION THROUGH THE CONSTITUTION, KENYAN JURISPRUDENCE AND THE AFRICAN UNION’S CONVENTION ON PERSONAL DATA PROTECTION AND CYBERSECURITY:.....</b>	<b>75</b>
<b>Introduction:.....</b>	<b>75</b>
1. Constitutional Provisions and the Data Protection Agenda:.....	75
1. The protection of fundamental rights:.....	75
2. Jurisdiction: .....	77
2. Petition No. 503 of 2014: An analysis of the interaction of the Kenyan legal regime and emergent, data-centric technologies: .....	78
A. Introduction:.....	78
B. The Court’s Determination: .....	81
3. The African Union Convention on Personal Data Regulation and Cybercrime: Insights into the imminent African Data Protection Regime: .....	92
1. Introduction:.....	92
2. The principles of data protection regulation present in the AU Convention on Personal Data Protection and Cybercrime:.....	93
<b>CHAPTER FIVE: CONCLUSIONS AND RECOMMENDATIONS:.....</b>	<b>101</b>
<b>A. Recommendations: .....</b>	<b>101</b>
1. Data Transfers & Their Regulation: .....	101
2. Lessons from the current data protection reform in the European Union:.....	105
<b>B. Conclusion:.....</b>	<b>108</b>
<b>BIBLIOGRAPHY: .....</b>	<b>110</b>
BOOKS:.....	110
JOURNAL ARTICLES.....	110
WEB SOURCES: .....	110



## **CHAPTER ONE: RESEARCH PROPOSAL.**

### **Introduction:**

Cloud computing, in its simplest definition, can be defined as a way of delivering computing resources as a utility service via a network, typically the Internet, scalable up and down according to user requirements.<sup>1</sup> As such, the cloud may prove to be as disruptive an innovation as was the emergence of cheap electricity on demand centuries ago. Such computing resources may range from raw processing power and storage, such as servers or storage equipment, to full software applications. Users can rent IT resources from third parties when needed, instead of purchasing their own, thus “turning capex into opex” (turning capital expenditure into operating expenditure). The latter, particularly in Africa has been fundamental in the adoption and proliferation of cloud services within its populace.

At the heart of the technical development of cloud technology, however, lies the true benefit of its implementation within modern society, a resource of our time whose wise utilisation continues to leapfrog human advancement in new and fantastic ways; data. Data is the lifeblood of technological innovation in the modern society, as it enables manufacturers to actively assess market needs, to wisely invest funds in the fulfilment of viable solutions and finally to fulfil those needs in a profit-maximised manner. The utility of these products by the public ultimately carry significant trickle-down benefits as the efficiency of numerous service and product providers are boosted tremendously by the adoption of these technologies, which ultimately impact the society as a whole through the enjoyment of better products and services.<sup>2</sup> The value chain of data, and its ability to maximise business profitability has led to the development and widespread adoption of data mining and analytics by local and multinational companies alike. Moreover, the highly disruptive nature of the implementation of data-centric business strategies has motivated firms to adopt and utilise the power of data in order to provide innovative Sand

---

<sup>1</sup> Millard Christopher; *Cloud Computing Law*, Oxford University Press, Great Clarendon Street, Oxford , United Kingdom, 2013 ,p. 1.

<sup>2</sup><http://webcache.googleusercontent.com/search?q=cache:http://www.laits.utexas.edu/~norman/BUS.FOR/courses/mat/Alex> According to research on data mining in the University of Austin, Texas, data-centric business models tend to be more successful than classic business models in the modern day and age.(Accessed on 5/11/2015)



wholesome solutions in accordance with their consumers' tastes (who have developed a rather discerning appetite) or face elimination by competitors who have adopted proper digital strategies in order to fulfil such market needs. This notion was particularly well-captured by John Chambers, former CEO of Cisco Systems Inc, when he stated that , according to research carried out by his company, only 40% of current global businesses today would survive the data-centric digital revolution that was occurring in the modern age. All companies alike, according to Cisco's findings, are thus faced with a stark ultimatum; to either disrupt or get disrupted.<sup>3</sup>

Despite the various socio-economic benefits attached to the utilisation of data as a resource, the practice of data mining and data analytics poses significant questions regarding the constitutional rights and freedoms accorded to individuals from whom this data is derived. In achieving the immense potential which data possesses, analysing and mining data indiscernibly could lead to notable violations of the constitutional right to privacy, as well as the consumer rights of protection against undue economic exploitation by producers. There is thus, a necessity to protect and legislate for the need to differentiate, collect and process data from numerous individuals by data processors in a transparent and equitable manner. Thus, the function of data protection law in the modern society can be seen to be the fundamental role of establishing a balance between the commercial needs of various data-centric operations in modern-day corporate establishments while protecting the fundamental rights and freedoms of various individuals as guaranteed by each jurisdiction's Constitution.

#### **JUSTIFICATION OF THE STUDY:**

Centrally, the justification of this study is founded upon the significant integration of cloud-based technologies into the social, economic and political activities of African individuals in the modern society. The proliferation of cloud-based technologies within the African populace has been fuelled by certain economic and infrastructural realities affecting numerous States in the continent.

---

<sup>3</sup> John Chambers' final key note address in Cisco Live 2015, asserted the numerous points made in this paragraph. See video link as attached here. (<http://www.youtube.com/watch?v=ujBLqLFNr0s>)



The first of these is the vast broadband coverage within the region. About 87% of the African region has broadband connectivity, thus enabling the adoption of new mobile technologies at an accelerated pace.<sup>4</sup> Fundamentally, the latter is influenced by another reality; this regards the price and availability of mobile devices within Africa. According to UNDP, 1 out of every 3 Africans has a mobile phone. The latter is due to the introduction of cheaper versions of mobile devices by prominent mobile technology manufacturers such as Apple, Samsung and Huawei; whose shrewd business strategies have enabled Africans to enjoy the utility benefits of technology at a reduced cost. In a survey carried out by The Guardian, the current trend of the consumption of mobile technologies within the African populace is only the beginning, as the rate of mobile consumers is expected to rise twenty-fold in the next five years, with the rise of internet-based services continuing at a similar trend.<sup>5</sup>

Economically, the impact of cloud-based technologies run on mobile devices is tremendous, particularly within the Kenyan jurisdiction. This situation is best illustrated by the immense success story of the M-PESA mobile money transfer service. This award-winning product is run by the Nairobi-based Safaricom Company. Nearly a decade after its launch, M-PESA has transformed economic interaction in Kenya. Its success reshaped Kenya's banking and telecom sectors, extended financial inclusion for nearly 20 million Kenyans, and facilitated the creation of thousands of small businesses. M-PESA has been especially successful in reaching low-income Kenyans: new data indicates that the percentage of people living on less than \$1.25 a day who use M-PESA rose from less than 20 percent in 2008 to 72 percent by 2015. Groups that typically have limited access to formal financial services have benefited from the financial products offered through M-PESA. In particular, its short-term Pay Bill Account service allows users to fundraise for a variety of purposes, including expenses relating to medical needs, education, and disaster relief.<sup>6</sup> M-PESA has also empowered business creation—many small companies rely on M-PESA for nearly all transactions, or provide a service that is a derivative of the platform itself. This has significantly empowered the SME economy which is the economic

---

<sup>4</sup> Erick Hersman, iHub, *Mobile Technologies in Africa* (2013)

<sup>5</sup><http://www.vodafone.com/business/global-enterprise/invisible-infrastructure-the-rise-of-africas-mobile-middle-class-2013-08-22> (Accessed on 5/11/2015)

<sup>6</sup><http://www.theguardian.com/technology/2011/jul/24/mobile-phones-africa-microfinance-farming> (Accessed on 5/11/2015)



backbone of the Republic of Kenya. Socially, cloud-based technologies have taken centre stage in the global and local digital market, social networking platforms such as Twitter, Whatsapp, Facebook and Instagram are part and parcel of the social undertakings of the metropolitan and rural populace, who seek to communicate and interact with each other through the internet. Subsequently, the social aspects of technology have enabled a growth in the political participation of citizens in African States, particularly among the youth who have been exposed to multiple world views, as well as global news, courtesy of the Internet.<sup>7</sup> An interesting political consequence of the adoption of these technologies is the ability accorded to the public that enables it to publicly scrutinise government activities and reward such actors with positive feedback that enables the regime's agenda, or with politically scathing negative feedback regarding the regime's institutional or systemic failures in the provision of public services to Her people. Bearing in mind the history of corruption and malpractice in Africa, technology's contribution to the emancipation of the public from the oppression by State kingpins may have played a fundamental role in its widespread adoption in the continent's society.<sup>8</sup>

With the growth of cloud users throughout the Continent comes the inevitable generation of petabytes of data regarding the personal relationships and commercial undertakings of billions of African users. Hidden within this data, is the immense opportunity to improve the standard of life of the largely impoverished African populace, as well as data-centric solutions to numerous economic problems faced by the various regions of Africa, such as drought, famine, disease, illiteracy and poor governance. However, there also exists an impending threat to the national security of States, on account of this growth of data presence within Africa. Personal data regarding the growing number of data subjects across the Continent could be used to harm the individuals themselves in agonising ways. As the digitisation of products and services grows, the users of such services submit sensitive information, regarding their health, lifestyles and business transactions, which when leaked or made public could inflict great harm to the reputation, economic relationship or overall health of the person so involved. Moreover, with the rise of

---

<sup>7</sup><http://www.theguardian.com/technology/2011/jul/24/mobile-phones-africa-microfinance-farming>(Accessed on 5/11/2015)

<sup>8</sup><http://www.theguardian.com/technology/2011/jul/24/mobile-phones-africa-microfinance-farming>(Accessed on 5/11/2015)





radicalism and terrorism in the 21<sup>st</sup> Century, terrorists may be able to set out elaborate schemes in order to wreak havoc on States, based on intelligence derived from unprotected data sources. Deficiencies in legislation regarding data protection may also perpetuate cybercrime, as criminals seek to exploit cloud infrastructure to create international platforms that provide illegal products and services such as child pornography, transborder money transfers and payment schemes for the trafficking of illegal goods. Nature abhors a vacuum, and according to recent research carried out by the International Telecommunication Union, African legislators seem largely unprepared for the numerous threats that data abundance poses to their sovereignty and national security.

**STATEMENT OF THE PROBLEM:**

Within European jurisdictions, legislation has played the essential role of safeguarding the data of their citizens through various elaborate mechanisms. The assessment of these legislative safeguards could help design viable and innovative legal solutions to the miasma of conflict which data integrity in the cloud could be for African courts.

The enactment of the African Union's Convention on Cybercrime and Personal Data Protection may seem to remedy numerous data protection concerns, but the question remains as to whether the Convention anticipated the development of cloud technology and its proliferation in Africa. If not, the latter could prove to be one of the largest hindrances to the growth of e-commerce and foreign investment in emerging African businesses.

The widespread use of indigenous cloud-based technologies, such as Sportpesa and M-Pesa within the Kenyan jurisdiction could lead to differentiated and unique legal considerations as regards their use by Kenyan citizens. It is crucial that Kenyan legislation offer guidance regarding the numerous legal risks posed by such technologies, as failure to do so will constitute a breach of the Kenyan Constitution of 2010, which necessitates the ardent protection of consumer rights and right to privacy.



**STATEMENT OF THE OBJECTIVES:**

This paper will endeavour to achieve the following objectives:

- This paper will seek to investigate the numerous global standards which govern the collection and use of personal data in the cloud, in order to incorporate such tenets into the Kenyan jurisdiction's practices.
- The paper will objectively analyse the European Union's Data Protection regime in order to infer any favourable data protection regulations which could further supplement the African Union Convention on Cybercrime and Personal Data Protection and vice versa.
- This paper will look into the Kenyan regulations on data protection and will seek to analyse whether the global standards of data protection, such as the OECD Guidelines on Data Protection have been incorporated into local statutes, as well as the principles proposed by the African Union Convention on Cybercrime and Personal Data Protection.
- This paper will seek to make appropriate recommendations regarding the data protection regime in Kenya, in accordance with its findings and research.

**AN INTRODUCTION TO DATA PROTECTION: THE CONCEPT OF PROCESSING AND DATA PROTECTION ACTORS:**

**1. The concept of processing:**

Much of what has been said above is predicated on the notion that data is processed. It is now appropriate to consider what forms of activity can be classed as constituting processing. The European Data Protection Directive provides here that processing includes any operation or set of operations which is performed upon *personal data*, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation,



use, disclosure by transmission, dissemination or otherwise making available<sup>9</sup>, alignment or combination, blocking, erasure or destruction.<sup>10</sup>

The United Kingdom 1998 Data Protection Act's definition differs slightly in terminology, largely because of the need to make separate provision for the treatment of non-automated or manual processing.<sup>11</sup> It provides that 'processing', in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including organisation, adaptation or alteration of the information or data; retrieval, consultation or use of the information or data; disclosure of the information or data by transmission, dissemination or otherwise making available; or alignment, combination, blocking, erasure or destruction of the information or data.<sup>12</sup> Linked to this is a definition of the word data, as:

*... is being processed by means of equipment operating automatically in response to instructions given for that purpose; (b) is recorded with the intention that it should be processed by means of such equipment; or (c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system.*<sup>13</sup>

The term 'relevant filing system' is designed to extend the legislation to certain forms of manual filing systems and will be considered separately below. It will be noted that the scope of the definition is extremely broad. It might be suggested, with little element of exaggeration, that whilst the act of dreaming about data will not constitute processing, any further activities will bring a party within the scope of the legislation.<sup>14</sup> Although not yet at issue before a United Kingdom court, the question of what acts constitute processing was raised before the European Court in *Bodil Lindqvist*.<sup>15</sup> An initial issue concerned the question of whether the mention of a

---

<sup>9</sup> Lloyd. J. Ian, *Information Technology Law, Sixth Edition*. published in Oxford University Press (2012), Great Clarendon Street, United Kingdom, p. 49

<sup>10</sup> Article 2(b), Data Protection Directive, 95/46/EC

<sup>11</sup> Lloyd. J. Ian, *Information Technology Law, Sixth Edition*, p.49

<sup>12</sup> Section 1(1), *The United Kingdom Data Protection Act, 1998*.

<sup>13</sup> Section 1(1), *The United Kingdom Data Protection Act, 1998*.

<sup>14</sup> Lloyd. J. Ian, *Information Technology Law, Sixth Edition*, p.49

<sup>15</sup> *Bodil Lindqvist*, Case 101/01, [2004] QB 1014



person on a web page constituted processing of personal data as defined in the Data Protection Directive.<sup>16</sup> Two issues arose in this context: first, whether the data on Mrs Lindqvist's web page included personal data. The court's reply was unequivocal:

*The term undoubtedly covers the name of a person in conjunction with his telephone coordinates or information about his working conditions or hobbies.<sup>17</sup>*

Equally clear was the court's determination that processing had taken place. The Swedish government argued for a broad approach, suggesting that 'as soon as personal data are processed by computer, whether using a word-processing programme or in order to put them on an Internet page, they have been the subject of processing'. Although Counsel for Mrs Lindqvist argued that something more was needed beyond compilation of what was effectively a word-processed document and that only metatags and other technical means used to assist with the compilation of indexes and retrieval of information would suffice, the court agreed with the Swedish government's submission:

*According to the definition in Article 2(b) of Directive 95/46, the term processing of such data used in Article 3(1) covers any operation or set of operations which is performed upon personal data, whether or not by automatic means.<sup>18</sup>*

Although all forms of processing are potentially covered by the Data Protection Directive,<sup>19</sup> the most stringent controls apply in the case of processing by automatic means. It is arguable that any use of a computer to create a document comes within the scope of this criterion, as there is no direct physical link between the author pressing a key and a letter or symbol appearing on the screen. The act of loading a page onto a web server involved a number of operations, some at least of which are performed automatically.

---

<sup>16</sup> Directive 95/46/EU

<sup>17</sup> *Bodil Lindqvist*, Case 101/01, [2004] QB 1014, para. 24.

<sup>18</sup> *Bodil Lindqvist* para. 25

<sup>19</sup> Directive 95/46/EU



## **2. Data Protection Actors:**

### **A. Data Controllers:**

Data controllers are subject to the most extensive forms of control under the Data Protection Act and Directive. The Directive provides that: 'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law.<sup>20</sup> The Data Protection Act provides that a party will be classed as a data controller when it: . . . (*either alone or jointly or in common with other persons*) *determines the purposes for which and the manner in which personal data are, or are to be processed.*<sup>21</sup>

In the case where data are processed only for purposes required by statute, for example the compilation of an electoral roll, the agency charged with conducting the work will be classed as the data controller.<sup>22</sup> The key element of the above definitions relates, with the exception of the performance of statutory functions, to the ability to determine the nature and extent of the processing which is to be carried out. It is quite possible for persons to be classed as data controllers even though they do not own a computer. An example might concern the owner of a small business who records details of transactions on pieces of paper which are stored in the archetypal shoebox. Once a year, the shoebox may be collected by an accountant, who transfers the data to computer in order to prepare a set of accounts<sup>23</sup>. Assuming that some of the data in the accounts relate to individual creditors and debtors, all the criteria necessary for the application of the legislation will be satisfied and, doubtless much to their surprise, the business person will be classed as a data controller. In such a situation, the accountant will also be so regarded, the Divisional Court confirming *in Data Protection Registrar v Griffin*,<sup>24</sup> a case brought under the Data Protection Act 1984, that anyone who processed data on behalf of clients

---

<sup>20</sup> Article 2(d), Data Protection Directive, 95/46/EU.

<sup>21</sup> Section 1(1), United Kingdom's Data Protection Act, 1998.

<sup>22</sup> Lloyd. J. Ian, *Information Technology Law, Sixth Edition*, p.51

<sup>23</sup> Lloyd. J. Ian, *Information Technology Law, Sixth Edition*, p.52

<sup>24</sup> *The Times*, 5 March 1993



would be regarded as a data user (now controller) when he or she possessed any control or discretion concerning the manner in which the processing was carried out. A similar result is postulated in the Recitals to the Data Protection Directive:

*... where a message containing personal data is transmitted by means of a telecommunications or electronic mail service, the sole purpose of which is the transmission of such messages, the controller in respect of the personal data contained in the message will normally be considered to be the person from whom the message originates, rather than the person offering the transmission services; whereas, nevertheless, those offering such services will normally be considered controllers in respect of the processing of the additional personal data necessary for the operation of the service.*<sup>25</sup>

**B. Data Processors:**

As in the example given above, some data controllers may seek to have processing carried out on their behalf by a third party. This was perhaps more prevalent in the early days of computing than is the case today, although one aspect which remains significant is where undertakings make arrangements as part of a disaster recovery plan, to obtain access to external processing facilities in the event of some interruption to service.<sup>26</sup> Mirroring once again the terminology of the Data Protection Directive,<sup>27</sup> the Data Protection Act 1998 utilises the term 'data processor' which encompasses:

*... any person (other than an employee of the data controller) who processes the data on behalf of the data controller.*<sup>28</sup>

The phrase in brackets was included to avoid the possibility that employees engaged in processing in the course of their employment might be regarded as data processors. Given the expanded definition of processing adopted in the 1998 Act, it will be the case that any other

---

<sup>25</sup>Directive 95/46/EC, Recital 41.

<sup>26</sup>Lloyd. J. Ian, *Information Technology Law, Sixth Edition*, p.51

<sup>27</sup> Directive 95/46/EC.

<sup>28</sup> Section 1(1), UK Data Protection Act (1998)



person who collects data for the controller, perhaps by conducting market research surveys using pen and paper, will be classed as a processor. Although a wide range of persons may be classed as data processors, the requirements imposed on them are limited. Data processors will not be subject to the notification requirements,<sup>29</sup> whilst, in respect of the requirement to maintain appropriate security (now found in the seventh principle), the onus is placed upon the data controller for whom processing is conducted. The controller is responsible for selecting a processor who can provide satisfactory guarantees regarding security. A written contract must also be entered into obliging the processor to act only on instructions from the controller in respect of the processing carried out, and also to comply with the requirements of the seventh principle.<sup>30</sup> Further, it is only the data controller who may be liable to compensate data subjects for losses arising from processing.<sup>31</sup>

#### C. Data Subjects:

A data subject is 'an individual who is the subject of personal data'.<sup>32</sup> It would be a unique individual who is not to be classed as a data subject many times over. In contrast to the situation with data controllers and processors, where the focus is very much on the obligations imposed under the legislation, for data subjects, the purpose of the statute is to confer rights. The most important right for data subjects is undoubtedly that of obtaining access to data held by controllers and of securing the correction of any errors contained therein.<sup>33</sup>

#### **Research methodology:**

---

<sup>29</sup>Section 17, which provides for notification, refers only to this obligation being imposed upon data controllers, UK Data Protection Act`

<sup>30</sup>Schedule 1, Pt. 2, para. 12, UK Data Protection Act.

<sup>31</sup>Section 13

<sup>32</sup>Section 1(1). Section 1(4) contains the equivalent provision in the Data Protection Act 1984.

<sup>33</sup>Lloyd. J. Ian, *Information Technology Law, Sixth Edition*, p.56.



During the duration of my research, I will use the following items in order to achieve the numerous objectives set by this proposal:

- Published articles
- Journals
- Stellar dissertations, theses and relevant academic material

### **Chapter Breakdown:**

In order to properly fulfil the objectives set out in this paper, the material will thusly be ordered into the following criteria:

#### **1. Chapter One: Research Proposal.**

This will involve the background to the problem, a statement of the problem, and the research objectives set out to be fulfilled by this paper. Further, this chapter will enumerate on the numerous working concepts and definitions and terms as selected by the author in the construction of this paper.

#### **2. Chapter Two: Fundamental concepts and theories regarding Cloud Computing and the Emergence of data protection policy in the global digital market:**

This chapter will deal with the introduction to fundamental technical aspects of cloud computing and its impact upon the legislation of the cloud deployment practice digital market. The second chapter will also outline the emergence of data protection regulation in modern society, as a historical approach to the subject is essential to determining as to whether data protection fulfils the roles it is meant to in society today, or whether it has failed in legislating against data-centric innovations such as cloud technology.

#### **3. Chapter Three: Data Protection Derived From The European Union And Their Application on Cloud-based Technologies:**





This chapter will entail detailed insights into the various principles and tenets of data protection regulation within Europe, with a focus on the jurisprudence and statutes sourcing from the United Kingdom. The latter has been selected as a point of emphasis by the author as it is the cradle of the common law, and has immense influence in the development of legislation and *ratio descedendi* in other common law jurisdictions such as Kenya. The outcome of this chapter is to successfully eke out the essential concepts of data protection regulation in these jurisdictions in order to juxtapose them in relation to Kenyan data protection regulation.

**4. Chapter Four: Analysing The Present Data Protection Framework Within The Kenyan Jurisdiction Through The Constitution, Kenyan Jurisprudence And The African Union Convention On Personal Data Protection And Cybersecurity:**

This chapter will investigate current data protection regulation within Kenya, while referring to the principles present in the African Union Convention Regarding Personal Data Protection and Cybersecurity. This will enable a concrete comparison with the European data protection regime, and will ultimately reveal the gaps that African legislation has/ has not anticipated, in comparison with the European data protection regime. This chapter may also highlight the areas that the African legislation has surpassed European and English jurisprudence.

**5. Chapter Five: Conclusions and Recommendations:**

The final chapter will regard numerous recommendations from the author which may serve data protection regulators in the Kenyan jurisdiction, as well as insight regarding the emerging issue of transborder data transfer and its effect on current global data protection legislation.



**CHAPTER TWO: FUNDAMENTAL CONCEPTS AND THEORIES REGARDING CLOUD COMPUTING AND THE HISTORY OF THE EMERGENCE OF DATA PROTECTION POLICY IN THE GLOBAL DIGITAL MARKET:**

**A. Cloud Computing:**

**1. Introduction:**

Cloud computing can technically be defined as an arrangement whereby computing resources are provided on a flexible, location-independent basis that allows for rapid and seamless allocation of resources on demand.<sup>34</sup> Typically, cloud resources are provided to specific users from a pool shared with other customers with pricing, if any, often proportional to the resources used. The delivery of cloud services often depends on complex, multi-layered arrangements between various providers.

Many permutations are possible, but cloud computing activities are often described as falling into one or more of the following three service categories:

1. **Infrastructure as a Service (“IaaS”):** raw computing resources, such as processing power (“compute”) and storage.<sup>35</sup>
2. **Platform as a Service (“PaaS”):** platforms for developing and deploying software applications.<sup>36</sup>
3. **Software as a Service (“SaaS”):** end-user applications.<sup>37</sup>

Cloud users may run, typically via web browsers, application software installed on remote servers which sends results to users over the Internet. This means that relatively simple devices, such as mobile phones or tablets, may be used to obtain access to vast computational resources.

The use of “as a Service” emphasizes a change in focus, from obtaining products or licenses to renting the use of resources as services. These service models sit on a spectrum from IaaS to PaaS to SaaS, rather than being separate or discrete types of cloud computing.

---

<sup>34</sup> Millard C., *Cloud Computing Law*, p.1

<sup>35</sup> Millard C., *Cloud Computing Law* p.2

<sup>36</sup> Millard C., *Cloud Computing Law* p.2

<sup>37</sup> Millard C., *Cloud Computing Law* p.2



Generally, IaaS involves relatively low-level functionality for users, requiring greater user sophistication and expertise, including more hands-on, and micromanagement of resources. However, it affords the user more flexibility and fine control. SaaS provides high-level functionality, and generally requires less user technical expertise, but offers less user control. PaaS sits in the middle. Users are spared the need to manage raw processing/storage resources actively, and may focus on programming applications to be hosted via the service. Boundaries between them, particularly IaaS and PaaS, may blur; IaaS providers are increasingly offering high level functionality. The latter is best illustrated by the provision of software development kits for Java, mobile (Android, iOS), PHP, Python, Ruby and ASP.NET programmers by the Amazon Cloud Service Providers. PaaS, on the other hand offers lower-level detailed control.<sup>38</sup>

SaaS is the most commonly used type of cloud service, particularly among consumers, which is unsurprising as it generally requires the least technical know-how on the part of users, and enables users to process use of application software quickly without installing any specific software.

1) **Types of cloud deployment models:**

Cloud deployment models can be viewed in various ways but a widely used classification can be shown as follows:

- a) **Private Cloud:** This occurs where the relevant infrastructure is owned by, or operated for, the benefit of a single large customer or a group of related entities.<sup>39</sup>
- b) **Public Cloud:** This occurs where infrastructure is shared among multiple users using the same hardware and/or software. An apt example of this model can be seen through the Facebook deployment model, as users utilize similar hardware and software resources in order to access the service. It is vital to note that private and public should not be equated with on and off premise. Infrastructure for cloud services may be located on users' premises, or at one or more external locations. Private clouds are not necessarily on

---

<sup>38</sup> Millard C., *Cloud Computing Law* p.3

<sup>39</sup> [http://www.cisco.com/en/US/solutions/collateral/ns340/ns517/ns224/state\\_of\\_alaska\\_cs.pdf](http://www.cisco.com/en/US/solutions/collateral/ns340/ns517/ns224/state_of_alaska_cs.pdf) (Accessed on 3/11/2015); the US State of Alaska contracted Cisco to deploy their private cloud service to optimize their agencies' efficiency



premise; the infrastructure/resources used could be managed, even owned, by a third party, but dedicated to the user concerned. Public clouds, however, are generally off-premise.

- c) **Community Cloud:** This occurs where infrastructure is owned by, or operated for, and shared among a specific group of users with common interests, such as US government bodies and the financial services industry. An example of the former is the deployment of the Microsoft Office 365 SaaS as a ‘multi-tenant service that stores US government data in a segregated community cloud.’ A lucid illustration of the adoption of the community cloud in the financial services industry can be shown by the NYSE Euronext’s Capital Markets Community Cloud for financial services (launched in 2011 in partnership with storage provider EMC and virtualization firm VMWare), which offers applications and services to customers via its ‘own app store’, computing on-demand services, and connections to NYSE Euronext’s global trading network, including a market data feed.<sup>40</sup>
- d) **Hybrid Cloud:** This deployment model involves a mixture of the above, for example, an organization which a private cloud may ‘cloud burst’ processing activities to a public cloud for ‘load balancing’ purposes during times of high demand.<sup>41</sup>

## 2. The Cloud Supply Chain: Key Concepts:

In order to comprehend the various parties involved in any given cloud deployment model, as well as the numerous legal risks present in the collection and analysis of data in any given cloud, it is key to unravel its cloud supply chain.

The cloud supply chain is intricate, and its complexity is differentiated by the type of cloud service provided by the vendor. One cloud service may combine hardware and/or software components from different suppliers or providers. Also cloud services may be combined or layered.<sup>42</sup>

---

<sup>40</sup> Millard C., *Cloud Computing Law* p.3

<sup>41</sup> Nati Shalom, ‘*What is Cloud Bursting?*’, <http://www.cloudcow.com/what-cloud-bursting> (Accessed on 3/11/2015)

<sup>42</sup> Millard C. *Cloud Computing law*, p. 14



A) Combining Components:

Cloud services ultimately employ physical infrastructure; equipment housed in physical locations, typically data centres. The data centre ecosystem may involve different players providing physical space, equipment (whether servers, storage or networking), software infrastructure and services and ancillary services.<sup>43</sup> Cloud platforms used as software infrastructure for cloud services may be proprietary or open source, hosted-only or available as installable software, and may not necessarily involve virtualization. Cloud service providers need not use their own cloud platforms or application software. Therefore, the owner, operator, manager, and user of a physical or software component may be different entities.

As a concrete illustration, a person X may buy or lease a dedicated data centre, or rent space in a third party's data centre where others also rent space ('colocation'). X could buy or rent storage servers or storage devices from third parties. Servers and other equipment could be dedicated to X, or shared with others. X might manage 'its' servers itself, with only its own employees having access to them, for example in a locked cage or room, perhaps with biometric entry for safety, and so on. Or, X might use a third-party service provider to help run and maintain its servers. On those servers, X could install a proprietary or open-source cloud platform.<sup>44</sup> Some suppliers even sell physical servers with open-source or proprietary cloud software infrastructure pre-installed. X could offer the use of its cloud infrastructure to others as IaaS<sup>45</sup>. Or, X could build its own PaaS platform on this infrastructure, to develop and host its own applications for private cloud, or to offer PaaS services to others. PaaS platforms, whether stand-alone or built on existing IaaS platforms, may also be installable on X's equipment, for X's own use or for offering to others as hosted services.<sup>46</sup> Physical and software infrastructure could be managed by X, or a third party on its behalf, such as a systems integrator. X might have a separate consultancy, or other services

---

<sup>43</sup> Millard C. *Cloud Computing law*, p. 14

<sup>44</sup> According to C. Millard in *Cloud Computing Law*, p.14, Canonical's Ubuntu Enterprise Cloud, which itself leverages OpenStack. This illustrates that even cloud platform software is not a single concept; there may be different kinds at different levels, for example, with more user functionality added, such as with Ubuntu Cloud.

<sup>45</sup> For example, European telecommunications and managed service provider Colt uses VMWare's vCloud platform to offer public and private cloud services as 'virtual data centres' in Colt's physical data centre, and Colt's physical data centres, and Colt also provides connectivity for those services.

<sup>46</sup> Millard C., *Cloud Computing Law*, p.14



contract, with an integrator to help it set up, manage or support its cloud.<sup>47</sup> X could install, on its own or third-party cloud infrastructure, application software it developed internally, or licensed from third parties. It could use these applications internally, as private cloud, or offer them as a service to others, as a SaaS provider.<sup>48</sup> These illustrate that many combinations are possible, and users may not necessarily know how a cloud service has been put together or who supplies provides or operates different components.

Users may also combine different cloud providers' services. Ancillary support for primary cloud services includes analytics, monitoring, and cloud-based billing systems. SaaS across different providers is increasingly integrated. Providers may use third-party cloud security providers, and integrate applications with, or support, 'non-cloud' components.<sup>49</sup>

Cloud use is becoming increasingly sophisticated and continuously widespread. With traditional IT, organizations may install and operate different applications, while with cloud, customers increasingly integrate different cloud applications and support services, with each other and with legacy internal systems.

B) Layers or chains of cloud services:

Cloud computing often involves a combination of 'layers' of services and such layering may not be transparent to users. The classification of a service depends on exactly which layers and actors are under consideration. For example, a customer of Dropbox may consider that they obtain a SaaS storage device from Dropbox. However, from the perspective of Dropbox, which built its SaaS service on Amazon's IaaS infrastructure, Amazon provides an IaaS service, which Dropbox uses to offer SaaS to its own consumers. Thus, Dropbox is both a cloud user (of Amazon IaaS) and cloud provider (of SaaS storage, to its customers).<sup>50</sup>

Furthermore, as already mentioned, PaaS may be layered on IaaS, SaaS on PaaS or IaaS; triple layers are possible. Examples of these are as follows:

---

<sup>47</sup> Millard C., *Cloud Computing Law*, p.14

<sup>48</sup> Millard C., *Cloud Computing Law*, p.14

<sup>49</sup> Millard C., *Cloud Computing Law*, p.14

<sup>50</sup> Millard C., *Cloud Computing Law*, p.14



- 1) 'Unlayered' IaaS, such as Amazon Web Services, Rackspace, Go Grid, or Google Compute Engine.
- 2) 'Unlayered' PaaS, such as Google App Engine, Microsoft Windows Azure or Salesforce's Force.com
- 3) PaaS on IaaS, such as dotCloud, Engine Yard, or Heroku (all built on Amazon IaaS).
- 4) 'Unlayered' SaaS, for example social networking or sharing services such as Facebook and Flickr, webmail services such as Gmail or Outlook.com, and Salesforce's customer relationship management service.
- 5) SaaS on IaaS, such as Dropbox, or Mozy (both on Amazon IaaS); indeed, any SaaS service built on Amazon, such as location-based consumer SaaS service Foursquare.
- 6) SaaS on PaaS, such as any SaaS service built on App Engine or Azure.
- 7) SaaS on PaaS on IaaS; any SaaS service built on IaaS-based PaaS services such as dotCloud or Heroku.

This multiplicity of possible architectures for what appears, to the end user, to be a single cloud service, means that users may be dependent on several different providers and sub-providers, this results in an overall interdependency of cloud services in delivering certain cloud-based services to end users.<sup>51</sup> This was well illustrated in April 2011 when Amazon Web Services suffered an outage in its US East Region and SaaS providers who relied on Engine Yard and Heroku were adversely affected.<sup>52</sup> Different contractual arrangements for supply or provision of different components may also exist between different parties. Despite the potential importance for users of multiple dependencies, it is often difficult for users to know who is involved in 'hidden' service layers behind the direct provider, or to assess the risks of a hidden provider's service or equipment failing.

It is possible that a particular cloud user might be the only entity involved in a private cloud arrangement and might have direct control over every component of its cloud service 'stack'.<sup>53</sup> In almost all cases, however, cloud computing arrangements are a new way of sourcing different

---

<sup>51</sup>Millard C., *Cloud Computing Law*, p.16

<sup>52</sup> See <http://gigaom.com/cloud/more-than-100-sites-went-down-with-ec2-including-your-paas-provider> (Accessed on 3/11/2015)

<sup>53</sup>Millard C., *Cloud Computing Law*, p.16



IT resources from multiple providers and it is common for there to be complex relationships between users and providers and between providers and sub-providers.<sup>54</sup>

It is tempting to regard cloud computing as just a new form of outsourcing. Many commercial, legal and regulatory issues relevant to outsourcing do indeed apply to cloud computing. However, cloud computing has some fundamental characteristics that distinguish it from traditional outsourcing and which may affect the provider's or user's position in relation to risk management, contractual terms, and so on. In particular, there is considerable scope for confusion in dealing with layered services, particularly as regards assurances relating to security and sub-contractors.

C) Key differences from outsourcing:

Many current laws are difficult to apply to cloud arrangements because they do not cater adequately for the distinctive characteristics of cloud computing, including those arising from individual services' designs or from service type, particularly with public shared-infrastructure IaaS and PaaS. Hence, analyzing legal issues present within the cloud is not always straightforward.

The key differences between traditional outsourcing and cloud, which are important to bear in mind when considering legal issues are:

1. **Active agency versus passive resources for self-service usage:** Unlike with traditional outsourcing, public cloud providers do not act as agents that process data actively for users, but at most they passively store data which users choose to store and otherwise process on the provider's infrastructure, Providers may be active in maintaining and supporting the infrastructure and environment within which users process their data, but data processing is generally performed, not by providers, but by users operating the provider's resources on a self-service basis.<sup>55</sup>

---

<sup>54</sup> W. Kuan Hon and Christopher Millard, *Cloud Computing vs. Traditional Outsourcing-Key Differences*, Social Sciences Research Network (12/9/2012) , p.1

<sup>55</sup> Kuan Hon W and Millard C., *Cloud Computing vs. Traditional Outsourcing-Key Differences*, Social Sciences Research Network (12/9/2012) p.3





2. **‘Direction of travel’ and sequence of events:** In classic outsourcing, successive contacts ‘down the chain’ of processors may be easily tailored, from both timing and control perspectives. However, cloud involves the opposite sequence of events and ‘direction of travel’. Many cloud services are pre-packaged, standardized and commoditized services, which may be built on existing sub-provider services on sub-provider standard terms. The ‘sub-service’ in turn may be based on other services. A user chooses the provider and pre-built package that it think best meets its specific processing and other needs. It may, therefore, be difficult if not impossible to change particularly in different ways for different customers, sub-contracts between the provider and its sub-providers, because it has pre-built its service using standardized sub-service(s), rather than being commissioned to provide a service to order.<sup>56</sup>
3. **Standardized share infrastructure and environments:** Public cloud providers offer standardized, shared infrastructure and environments, often using relatively cheap commodity hardware, rather than tailoring them to each customer. Customization of services is sometimes possible, but costs extra time and money. Although IaaS affords a great degree of user control over individual resources, it is still provided in a standardized environment using the provider’s standardized system. Private cloud allows the most customization and control, especially if on a user’s own infrastructure and managed by the user, and if it is on third-party and/or managed by a third party, it is closest to traditional outsourcing. Traditional outsourced processing may use standardized infrastructure, sometimes at large scale, but it is unlikely to be shared to such an extent as in cloud. With shared infrastructure where users’ data are segregated, not through their being stored in separate physical equipment, but through their being separated ‘logically’ using software, users are reliant on the software separation being implemented properly and securely.<sup>57</sup>
4. **Knowledge:** In traditional outsourcing, processors are entrusted with the processing of specific data or types of data. In cloud, depending on the service, some providers may not

---

<sup>56</sup>Kuan Hon W and Millard C., *Cloud Computing vs. Traditional Outsourcing-Key Differences*, Social Sciences Research Network (12/9/2012) p.3

<sup>57</sup> Kuan Hon W and Millard C., *Cloud Computing vs. Traditional Outsourcing-Key Differences*, Social Sciences Research Network (12/9/2012) p.3



even know the nature of data (e.g. personal data) processed using their services, or how users are processing data, unless and until the provider chooses actively to access such data, assuming no encryption. In this sense, some providers are mere hosts renting out resources, and ought not to be treated in the same way as providers who access and utilize user data for their own purposes. Thus, ‘the cloud of the unknowing’ works both ways, users may not have much knowledge regarding the supply chain, but providers may not have much knowledge regarding data or processing either.<sup>58</sup>

### **B. Foundational concepts of data protection:**

Dictionaries and definitions seldom make compelling reading, but in the law an appreciation of basic concepts is key to understanding of a topic. Prior to considering substantive aspects of data protection, this section will consider in some detail the core concepts which define the scope of data protection legislation. A number of definitional terms are closely linked to form a knot almost Gordian in its complexity.<sup>59</sup> Any attempt to describe and analyse them is hindered by the fact that appreciation of the scope of one term presupposes to some extent understanding of others. In the absence of a sufficiently sharp sword, the following précis may serve as an introduction. The italicised terms will be subjected to more detailed analysis in the remainder of this paper:

*Data protection legislation applies where personal data (including sensitive personal data) relating to an identifiable individual (data subject) is subjected to certain forms of processing. The nature and extent of the processing will be determined by a data controller, although the actual processing may be carried out by a data processor operating under an outsourcing or similar contract with the data controller.*<sup>60</sup>

---

<sup>58</sup>Kuan Hon W and Millard C., *Cloud Computing vs. Traditional Outsourcing-Key Differences*, Social Sciences Research Network (12/9/2012) p.3

<sup>59</sup>Lloyd. J. Ian, *Information Technology Law, Sixth Edition*, p. 39

<sup>60</sup>Lloyd. J. Ian, *Information Technology Law, Sixth Edition*, p. 39



**The Emergence of Data Protection in Contemporary History:**

Initial legislative initiatives in the field occurred at the national level with the German state of Hesse adopting the world's first data protection statute in 1970.<sup>61</sup> The first national statute was the Swedish Data Protection Act adopted in 1973.<sup>62</sup> The fact that data protection laws were pioneered in these two countries may not be entirely a matter of coincidence, and also illustrates what might be classed as the positive and negative aspects of the system. In the case of Germany, there had been experience of the misuse of data by totalitarian governments, both under the Nazis and also looking eastward at the time to the Communist regime in the then East Germany.<sup>63</sup> In seeking to place limits on the ability of public and private sector bodies to process personal data, the law can be seen as acting primarily in a defensive manner. The Swedish situation was rather different. In this country there was no background of totalitarianism, but, a more than two-century long tradition of freedom of information, under which almost any item of information held by public bodies was considered to be in the public domain.<sup>64</sup> By conferring rights on individuals to access information held on any computer, data protection could be seen as extending some of the concepts of freedom of information into the private sector.<sup>65</sup>

Although the first data protection laws were enacted on a national basis, even prior to these measures, pressure had been exerted for international action in the field. In many respects, a comparison can be drawn with the first form of electronic data transfer made possible by the electric telegraph around the middle of the nineteenth century.<sup>66</sup> As national networks emerged, governments initially resisted international connectivity largely because of fears that because of the near instantaneous nature of telegraphic transmissions, messages against the national interest might be transmitted without the possibility for interception in transit which featured strongly with older postal systems of message delivery. Within a very few years, however, international transfer agreements were adopted, firstly, on a unilateral basis, then between regional groupings,

---

<sup>61</sup>Lloyd. J. Ian, *Information Technology Law*, Sixth Edition, p. 21

<sup>62</sup>Simitis, 'Reviewing Privacy in an Information Society', *University of Pennsylvania Law Rev*, Vol. 135, No. 3 (March, 1987), pp. 707-46.

<sup>63</sup>Simitis, 'Reviewing Privacy in an Information Society', *University of Pennsylvania Law Rev*, Vol. 135, No. 3 (March, 1987), , pp. 707-45

<sup>64</sup>Lloyd. J. Ian, *Information Technology Law*, Sixth Edition, p. 21

<sup>65</sup>Lloyd. J. Ian, *Information Technology Law*, Sixth Edition, p. 21

<sup>66</sup>Lloyd. J. Ian, *Information Technology Law*, Sixth Edition, p. 21



and, finally, from 1865, under the auspices of the International Telegraph Convention and Union, which formed the world's first international organization and laid the basis for the free transfer of data on a global basis.<sup>67</sup> In the data protection context, two concerns prompted international action. There were fears that national laws, which tended to have strong controls over the export of data might have a protectionist effect. Conversely, there were fears by those states that had adopted data protection legislation that national laws and policies could be circumvented by organizations sending data abroad for processing in countries (often referred to as data havens) which imposed few controls over processing activities.<sup>68</sup> As a more technical level, the 1970s also marked the period where developments in computers and communications technology rendered feasible a massive expansion in multinational organisations. Although these had existed for many years, activities tended to be restricted to activities such as car production, where assembly plants in different companies operated largely as independent freedoms. The year 1971 marked the opening of the first McDonald's restaurant in Europe.<sup>69</sup> The essence of this and similar businesses in the service sector is uniformity of product and identity across the globe. Such activities required the application of computer systems able to communicate across national boundaries. It was quickly recognised that international solutions were required in order to reconcile the interests of individual privacy with commercial interests. It was accepted that impossible burdens could be placed upon multinational enterprises should they be required to comply with differing standards in every country in which they acquired, stored, processed, or even transferred data. This indeed remains a problematic issue, with companies such as Google advocating global data/privacy protection standards in order to simplify their task of complying with laws on a global basis.<sup>70</sup> From the late 1960s, a range of international agencies have been active in the field of data and privacy protection. At the initial stages, the most prominent actors were the Council of Europe and the Organisation for Economic Cooperation and Development (OECD). The following sections will consider the major activities carried out under the auspices of these organisations. Brief attention will also be paid to work conducted under the auspices of the UN.

---

<sup>67</sup> Lloyd. J. Ian, *Information Technology Law*, Sixth Edition, p. 21

<sup>68</sup> Lloyd. J. Ian, *Information Technology Law*, Sixth Edition, p. 21

<sup>69</sup> <http://www.macdonald.com/history/the-first-European-outlet> > (Accessed on 4/11/2015)

<sup>70</sup> See, for example, <http://news.bbc.co.uk/1/hi/technology/6994776.stm> (Accessed on 4/11/2015)



International Data Protection Regimes:

**I. The Council of Europe**

In 1968, the Parliamentary Assembly of the Council of Europe addressed a request to the Committee of Ministers that they consider the extent to which the provisions of the European Convention on Human Rights safeguarded the individual against the abuse of modern technology.<sup>71</sup> The Assembly noted particular concern at the fact that the European Convention, together with its UN predecessor, the Universal Declaration of Human Rights, had been devised before the development and widespread application of the computer. Whilst identifying the dangers of computer abuse, the Assembly's report also drew attention to a paradox which remains largely unresolved to this day<sup>72</sup>. Data protection seeks to give an individual a greater measure of control over personal information and to place controls over the dissemination of this information. This approach may conflict with another individual's claim to be allowed access to information under the European Convention on Human Rights. Here it is provided that: 'everyone has the right to freedom of expression. This shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.'<sup>73</sup> The conflict is well illustrated in cases such as *Campbell v Mirror Group Newspapers*<sup>74</sup> and *Douglas v Hello!*<sup>75</sup> where celebrities clashed with newspapers and magazines over the publication of photographs and stories about them. In both cases, the disputes went to the House of Lords, which delivered judgment for the complainants by slender 3:2 majorities.<sup>76</sup> Acting upon the Assembly's report, two separate resolutions were adopted by the Committee of Ministers, dealing with the private and the public sectors. The differences between the two sets of recommendations are comparatively minor, and for both sectors it was recommended that national laws should

<sup>71</sup> In Lloyd J. Ian's *Information Technology Law* p. 24; he states:

'The linkage between data protection and notions of fundamental human rights remains significant with the recent European Charter of Fundamental Rights adopted in 2007 (but not applicable in the United Kingdom) providing in Article 8 that 'Everyone has the right to the protection of personal data concerning him or her.'

<sup>72</sup> Lloyd J, Ian, *Information Technology Law, Sixth Edition*, p. 24

<sup>73</sup> Article 10 of the European Court of Human Rights.

<sup>74</sup> *Campbell v Mirror Group Newspapers*[2004] UKHL 22 on appeal from [2002] EWCA Civ 1373 and [2002] EWHC 499 (QB).

<sup>75</sup> *Douglas v Hello* [2007] UKHL 21 on appeal from [2005] EWCA Civ 106 and [2005] EWCA Civ 595, [2005] EWCA Civ 861.

<sup>76</sup> Lloyd J, Ian, *Information Technology Law, Sixth Edition*, p. 24



ensure that legislation should require that personal data be obtained fairly, that it should be accurate and up to date, should be relevant and not excessive nor retained for longer than is necessary. The recommendations also provided for controls over the range of disclosure of data, the grant of subject access and the application of procedures to allow any errors in data to be corrected.<sup>77</sup>

In an effort to minimise restrictions on the free flow of information, and in the hope of preventing major discrepancies between the national data protection laws, the Council of Europe moved beyond its earlier recommendations to sponsor the Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data (hereafter, 'the Convention'). The Convention was opened for signature in January 1981 and was to enter into force when it was ratified by five Member States of the Council of Europe. This did not occur until October 1985. The Convention has been amended by an additional protocol, 'regarding supervisory agencies and transborder data flows', which was opened for signature in October 2001 and entered into force in July 2004. At the time of writing, forty-two countries have ratified the Convention and twenty-eight an additional protocol which strengthens the original provisions in the areas of transborder data flow. Although the Convention is open for signature by countries who are not members of the Council of Europe, to date, no non-member State has done so.<sup>78</sup> The view has been expressed by several United States commentators that the provisions of the Convention were motivated more by considerations of commercial expediency and economic protectionism than by a genuine concern for individual privacy. In the course of a meeting of the Committee of Experts, the United States observer contrasted the sectoral approach adopted in that country with the omnibus data protection legislation envisaged under the Convention, and concluded that:

*. . . the draft convention appears to regulate a function, that is, it appears to regulate automated or electronic data processing and what the automated data processing industry may do with records about individuals. To our mind the draft convention is, in essence, a*

---

<sup>77</sup>Resolution (73) 22, The Council Of Europe.

<sup>78</sup> This may be contrasted with the Council of Europe's Convention on Cybercrime , which has been signed by Canada, Costa Rica, Japan, Mexico, and South Africa, and signed and ratified by the United States



*scheme for the regulation of computer communications technology as it may be applied to personal data record-keeping. The establishment and exercise of individual rights and the privacy of the individual seem to be treated in a secondary fashion. I would note particularly that the word 'privacy' is rarely mentioned in the Convention and is not included in its title*<sup>79</sup>.

According to Ian. J. Lloyd, such criticism is unfounded.<sup>80</sup> In his opinion, the Convention, as with much of the Council of Europe's work, is deeply rooted in the human rights context and specifically in the European Convention of Human Rights and, indeed, as noted above, Article 8 of the European Union's Charter of Fundamental Rights provides that 'Everyone has the right to the protection of personal data concerning him or her.' There is thus a strong linkage between notions of privacy and data protection. In its Preamble, the Convention reaffirms the Council of Europe's commitment to freedom of information regardless of frontiers, and proceeds to prohibit the erection of national barriers to information flow on the pretext of protecting individual privacy.<sup>81</sup> This prohibition extends, however, only where the information is to be transferred to another signatory state. Impliedly, therefore, the Convention permits the imposition of sanctions against any non-signatory state, especially one whose domestic law contains inadequate provision regulating the computerised processing of personal data.<sup>82</sup> An intractable state could effectively be placed in data quarantine. The standards required of domestic laws are laid down in Chapter 2 of the Convention, and its requirements will be considered in detail, in the next chapter when considering the substantive aspects of data protection. In addition to the Convention itself, the Council of Europe has adopted a substantial number of recommendations concerning the interpretation and application of the Convention principles in particular sectors, and in processing for the purposes of particular forms of activity such as might be carried out by

---

<sup>79</sup>Text of United States Department of State telegram, quoted in *Transnational Data Report*, vol. 1, no. 7 (1978), p. 22.

<sup>80</sup>Lloyd J, Ian, *Information Technology Law, Sixth Edition*, p. 26

<sup>81</sup> Article 12(2) of the European Convention on Human Rights (ECHR)

<sup>82</sup> Lloyd, J. Ian, *Information Technology Law, Sixth Edition*, p. 26, The additional protocol referred to above was drafted to bring the Convention into line with the EU's Data Protection Directive. It provides that data may be transferred to an external state only if that state guarantees an adequate level of protection



police authorities or insurance companies.<sup>83</sup> Following an eight-year period of inactivity, a further recommendation on processing for the purposes of profiling was adopted in 2010.

**II. The Organisation for Economic Co-operation and Development (OECD):**

At much the same time as the Council of Europe began its work in the field of data protection, the topic also appeared on the agenda of the Organisation for Economic Cooperation and Development (OECD). The OECD was established by international convention in 1960 and, as its title suggests, is primarily concerned with facilitating cooperation between member states in order to promote economic development. This might be contrasted with the Council of Europe's emphasis on human rights. Unlike other international organisations, the OECD functions as something of a Members Club, with states wishing to join being required to satisfy the existing members as to their suitability. The OECD currently has thirty members almost exclusively from the developed world. Discussions regarding possible membership are ongoing with a number of countries, including Russia and China, and cooperative agreements are in force with about seventy countries,<sup>84</sup> ensuring that the organisation's influence extends far beyond its formal membership. A Council consisting of representatives of all the Member States is 'the body from which all acts of the organization derive'.<sup>85</sup> The OECD's work in what it has tended to refer to as the privacy protection field began in 1969 when a group of experts was appointed to analyse 'different aspects of the privacy issue, e.g. in relation to digital information, public administration, transborder data flows, and policy implications in general'.<sup>86</sup> A further group was established in 1978 under Mr. Justice Kirby, then Chairman of the Australian Law Commission. The United States representatives also played a prominent role in the group's activities and the resulting product in the form of a Recommendation to Member States concerning Guidelines on the Protection of Privacy and Transborder Data Flows was endorsed by the OECD Council in September 1980. It was part of the group's remit that its

---

<sup>83</sup> The text of all these instruments can be obtained from [http://www.coe.int/t/dghl/standardsetting/dataprotection/Legal\\_instruments\\_en.asp](http://www.coe.int/t/dghl/standardsetting/dataprotection/Legal_instruments_en.asp) (Accessed on 4/11/2015)

<sup>84</sup> [http://www.oecd.org/pages/0,3417,en\\_36734052\\_36761800\\_1\\_1\\_1\\_1\\_1,00.html](http://www.oecd.org/pages/0,3417,en_36734052_36761800_1_1_1_1_1,00.html) (Accessed on 4/11/2015)

<sup>85</sup> Article 7 of the ECHR

<sup>86</sup> [http://www.oecd.org/document/18/0,3343,en\\_2649\\_34255\\_1815186\\_1\\_1\\_1\\_1,00.html](http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html) (Accessed on 4/11/2015)





'work was to be carried out in close cooperation with the Council of Europe and the European Community'.<sup>87</sup> Although covering much the same ground as the Convention, the Guidelines can perhaps be seen as a common law-based approach to the issues, as opposed to the Convention which was drafted very much in line with the civil law tradition. It has been suggested that:

*In the final result, although substantially similar in core principles, the Convention and the Guidelines could be analogised, albeit in a rough fashion, to the civil and common law approaches, respectively. Common law systems proceed pragmatically, formulating the rules of legal behaviour as they acquire experience, while the civil law tradition tends to rely upon codification of rules in advance of action.*<sup>88</sup>

Again, whilst the Convention is a legally binding instrument, the Guidelines, as the terminology indicates, have no legal force. A further Declaration on Transborder Data Flows was adopted by the OECD in April 1985. This made reference to the fact that: Flows of computerised data and information are an important consequence of technological advances and are playing an increasing role in national economies. With the growing economic interdependence of Member countries, these flows acquire an international dimension.<sup>89</sup> It also indicated its signatories' intention to promote access to data and information and related services, and avoid the creation of unjustified barriers to the international exchange of data and information, seek transparency in regulations and policies relating to information, computer and communications services affecting transborder data flows, develop common approaches for dealing with issues related to transborder data flows and, when appropriate, develop harmonised solutions, consider possible implications for other countries when dealing with issues related to transborder data flows.<sup>90</sup>

It is clear from these objectives that commercial and trading interests provide at least as significant a force for action as do concerns for individual rights. Although the Declaration

---

<sup>87</sup>[http://www.oecd.org/document/18/0,3343,en\\_2649\\_34255\\_1815186\\_1\\_1\\_1\\_1,00.html](http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html) (Accessed on 4/11/2015)

<sup>88</sup> Kirsch I., *Legal Issues of European Integration* (1982), para 21 at p. 45

<sup>89</sup> Lloyd J. Ian, *Information Technology Law*, p. 28

<sup>90</sup> Kirsch I., *Legal Issues of European Integration* (1982), para 21 at p. 45



commits its member countries to conduct further work relating to specific types of transborder data flows, especially those accompanying international trade, marketed computer services, and computerised information services and intra-corporate data flows, no further measures have been adopted. In addition to its work in producing legal texts, the OECD has also sponsored the development of what is referred to as a privacy generator.<sup>91</sup> This online package is intended to be used by website developers and others to incorporate procedures and safeguards to ensure that sites operate in conformity with the principles laid down in the Guidelines.<sup>92</sup>

### **III. The Asia-Pacific Privacy Charter Initiative:**

At a rather less formal level than has occurred within Europe, considerable work has been carried out by a range of countries in the Asia-Pacific region (including the United States) who have established the Asia-Pacific Privacy Charter Council. Hosted at the Cyberspace Law and Policy Centre of the University of New South Wales, the Council is described as a 'regional expert group' which aims to: develop independent standards for privacy protection in the region in order to influence the enactment of privacy laws in the region, and the adoption of regional privacy agreements, in accordance with those standards.<sup>93</sup> The Council's work draws heavily on the APEC Privacy Framework drawn up by the Asia Pacific Economic Cooperation Organisation, the Preamble to which recognises the need for APEC economies to provide adequate protection for personal data in order to give individuals the confidence necessary to participate in electronic commerce, behaviour which almost of necessity requires the transfer of significant amounts of personal data.<sup>94</sup> Although still at a relatively early stage of development, the work provides further recognition of the global nature of privacy issues and the relationship between the development of electronic commerce and the effective protection of individuals' data.

---

<sup>91</sup> Lloyd J. Ian, *Information Technology law*, p.28

<sup>92</sup> [http://www.oecd.org/document/39/0,2340,en\\_2649\\_34255\\_28863271\\_1\\_1\\_1\\_1,00.html](http://www.oecd.org/document/39/0,2340,en_2649_34255_28863271_1_1_1_1,00.html) (Accessed on 4/11/2015)

<sup>93</sup> <http://www.bakercyberlawcentre.org/appcc/members.htm> (Accessed on 4/11/2015)

<sup>94</sup> [http://www.bakercyberlawcentre.org/ipp/apec\\_privacy\\_framework/index.html](http://www.bakercyberlawcentre.org/ipp/apec_privacy_framework/index.html) (Accessed on 4/11/2015)



**IV. The United Nations:**

On 20 February 1990, the United Nations' Economic and Social Council agreed to the Guidelines Concerning Computerised Personal Data Files.<sup>95</sup> These identify ten principles which, it is stated, represent the 'minimum guarantees that should be provided in national legislation'. The principles follow what might be regarded as the standard model, but there are two features of these Guidelines which justify mention at this point. First, they make provision for the application of the principles by international agencies,<sup>96</sup> bodies which might fall outside of national laws. Second, the UN Guidelines provide the option for the extension of the principles, both to manual files and to files held concerning legal persons.<sup>97</sup> In line with the Convention's approach, the UN Guidelines envisage the establishment of a supervisory agency providing that: the law of every country shall designate the authority which, in accordance with its domestic legal system, is to be responsible for supervising observance of the principles set forth above. This authority shall offer guarantees of impartiality, independence vis-à-vis persons or agencies responsible for processing and establishing data, and technical competence. In the event of violation of the provisions of the national law implementing the aforementioned principles, criminal or other penalties should be envisaged together with the appropriate individual remedies.<sup>98</sup> Recent years have seen attempts made to involve the UN more deeply in the data protection field. At the 2009 meeting of data and privacy protection commissioners, a proposal was endorsed encouraging the adoption of 'International Standards for the Protection of Privacy and Personal Data', allowing the development of a universal, binding legal document, which must be backed by the most extensive institutional and social consensus via the participation of the authorities and institutions guaranteeing data protection and privacy and representatives of both public and private entities and organisations.<sup>99</sup> In February 2010 the

<sup>95</sup> Available from <http://www.unhcr.org/refworld/publisher,UNGA,THEMGUIDE,,3ddcfaac,0.html> (Accessed on 4/11/2015)

<sup>96</sup> Available from <http://www.unhcr.org/refworld/publisher,UNGA,THEMGUIDE,,3ddcfaac,0.html> (Accessed on 4/11/2015), Part B.

<sup>97</sup> , Available from <http://www.unhcr.org/refworld/publisher,UNGA,THEMGUIDE,,3ddcfaac,0.html> (Accessed on 4/11/2015) para. 10

<sup>98</sup> Available from <http://www.unhcr.org/refworld/publisher,UNGA,THEMGUIDE,,3ddcfaac,0.html> (Accessed on 4/11/2015), para. 8

<sup>99</sup> <http://www.privacyconference2009.org/home/index-iden-idweb.html> (Accessed on 4/11/2015)



UN rapporteur on human rights made a call for the establishment of global privacy standards.<sup>100</sup> It is unclear when, or if, such an activity might be undertaken. The meeting of data and privacy protection commissioners, as the name implies, is dominated by representatives from countries which endorse the European model of protection with the establishment of dedicated supervisory authorities. As has been discussed, belief in the efficacy of this approach is not shared in other jurisdictions. There is also a gulf between countries which view data protection as essentially rooted in notions of human rights and those which see data protection as having an economic basis. In part this is based on notions of international data flows but at an internal level there is also often the belief that e-commerce and other online activities will flourish only if individuals have confidence that their data will not be misused.

**V. The European Data Directive & The Data Protection Act 1998:**

Until the early 1990s, the EU had played a peripheral role in the data protection arena. This could be ascribed to two main causes. First, the limited nature of the legislative competencies conferred by the establishing treaties gave rise to doubts as to whether, and to what extent, the EU was empowered to act in this field. Although the increasing importance of information as a commodity within the Single Market has provided a basis for European action, the exclusion of matters coming within the ambit of national security and, to a partial extent criminal and taxation policy, has served to limit the scope of the EU's intervention. A second factor influencing work in this field had been a reluctance on the part of the Commission to duplicate work being conducted under the auspices of the Council of Europe and in 1981, the Commission addressed a Recommendation to Member States that they sign and ratify the Convention.<sup>101</sup> By 1990, the Convention had been signed by all the Member States, but ratified only by six.<sup>102</sup> As will be described, the Convention establishes minimal standards but affords considerable discretion to signatories. A number of Member States, such as Germany and Sweden, had enacted laws which were considerably in advance of the Convention's minimum standards, whilst others, such as the United Kingdom, had openly

---

<sup>100</sup>[http://www.theregister.co.uk/2010/01/20/un\\_terror/](http://www.theregister.co.uk/2010/01/20/un_terror/) (Accessed on 4/11/2015)

<sup>101</sup>OJ 1981 L 246/31.

<sup>102</sup>Denmark, France, Germany, Luxembourg, Spain, and the United Kingdom.



indicated an intention to do the bare minimum necessary to satisfy obligations under that instrument. By 1990, Commission concern at the effect that discrepancies in the Member States' laws and regulations might have on inter-community trade resulted in proposals being brought forward for a Directive 'On the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data'.<sup>103</sup> The EU legislation, it was stated, would 'give substance to and amplify'<sup>104</sup> the provisions of the Convention. The objective of the proposal was stated to be to harmonise the data protection laws of the Member States at a 'high level'.<sup>105</sup> This approach was necessary because the Directive was adopted under the authority of Article 100a of the Treaty of Rome. This provides that the Community's law-making bodies may: adopt the measures for the approximation of the provisions laid down by law, regulation or administrative action in Member States which have as their object the establishing and functioning of the internal market. Reliance upon Article 100a has the further significant consequence in that any harmonising measures introduced under its authority have to secure 'a high level of protection'. Effectively, therefore, the Directive has to secure a level of protection equivalent to the highest currently available in the Member States. It is unclear how effective the Directive has been in this regard, with complaints being aired from countries such as Germany that implementation might dilute their existing regimes, especially in respect of transborder data flows. For the United Kingdom, implementation of the Directive required significant change to the Data Protection Act 1984, as well as its expansion. A Consultation Paper was published by the Home Office in March 1996, seeking views on the implementation of the Directive and indicating a preference for a minimalist approach to law reform: Over-elaborate data protection threatens competitiveness, and does not necessarily bring additional benefits for individuals. It follows that the Government intends to go no further in implementing the Directive than is absolutely necessary to satisfy the United Kingdom's obligations in European law. It will consider whether any additional changes to the current data protection regime are needed so as to ensure that it does not go

---

<sup>103</sup> OJ 1990 C 277/03.

<sup>104</sup> OJ 1990 C 277/03, para. 22

<sup>105</sup> Directive 95/46/EC, OJ 1995 L 281/31



beyond what is required by the Directive and the Council of Europe Convention. The Commission's proposal for a general Directive in the area of data protection was accompanied by a further proposal for a Directive 'Concerning the Protection of Personal Data and Privacy in the Context of Public Digital Telecommunications Networks'.<sup>106</sup> Following a five-year journey through the EU's legislative processes, the Data Protection Directive was adopted on 24 October 1995, with a requirement that it be implemented within the Member States by 24 October 1998. The Telecoms Directive—which for a while appeared to have been dropped from the legislative agenda—resurfaced, to be adopted in December 1997. It also required to be implemented by October 1998. The Telecoms Data Protection Directive proved to be a somewhat short-lived measure. In conjunction with a much broader reform of the European telecommunications regulatory regime, the Directive was replaced in 2002 by the Directive 'Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector'. This was required to be implemented in the Member States by 31 October 2003. Once again, aspects of the Directive proved short-lived with the adoption of Directive 2009/136/E, generally referred to as the 'Citizens' Rights Directive' in November 2009. This Directive requires to be implemented in the Member States by May 2011.<sup>107</sup> In January 1998 a Data Protection Bill was introduced in the House of Lords. Its progress through Parliament was relatively uncontroversial, with only one division being required throughout its parliamentary passage.<sup>108</sup> The major feature of the Bill's progress was the very large number of amendments tabled by the government—more than 200 in total. The Act received the Royal Assent on 16 July, although its entry into force was delayed pending the drafting of what proved to be seventeen items of secondary legislation and it was not until 1 March 2000 that the new legislation entered into force. In its failure timeously to implement the Data Protection Directive, the United Kingdom was joined by a majority of the Member States. Legal action was raised by the Commission against Denmark, France, Germany, Ireland, Luxembourg, and the Netherlands, alleging a continuing failure to implement the Directive,

---

<sup>106</sup> OJ 1990 C 277/12.

<sup>107</sup> Lloyd J. Ian, *Information Technology Law*, Sixth Edition, p. 28

<sup>108</sup> Directive 2002/58/EC, OJ 2002 L 201/37 (Privacy and Electronic Communications Directive).



although in the case of every state except Luxembourg, the belated implementation of the Directive resulted in the legal proceedings being abandoned.<sup>109</sup>

#### **VI. The Data Protection Act 1998:**

As an initial comment, it may be noted that the Data Protection Act 1998 is considerably larger than the 1984 legislation. The Data Protection Act 1984 has forty three sections and six Schedules; the 1998 statute has seventy-five sections and sixteen Schedules. To an extent greater than its 1984 precursor, the Act provides only a framework, with significant matters remaining to be determined by statutory instruments. Although this approach will allow easier modification and updating of the legislation than was possible with the 1984 Act, significant issues relating to the identification of those data controllers who may be exempted from the notification requirement are not covered in the Act. Given that the Data Protection Act 1998 is intended to implement a European Directive account has to be taken of the provisions of the latter. In *Campbell v MGN Ltd*<sup>110</sup> Lord Phillips of Worth Matravers MR stated that:

*In interpreting the Act it is appropriate to look to the Directive for assistance. The Act should, if possible, be interpreted in a manner that is consistent with the Directive. Furthermore, because the Act has, in large measure, adopted the wording of the Directive, it is not appropriate to look for the precision in the use of language that is usually to be expected from the parliamentary draftsman. A purposive approach to making sense of the provisions is called for.*

The European Court of Justice has also held in *Österreichischer Rundfunk*<sup>111</sup> that at least some of the provisions of the Directive are sufficiently precise to be relied upon directly by individuals within the Member States. The Data Protection Act 1998 extends significantly the area of the application of the legislation, including regulating some systems of manual records. In the accompanying Explanatory and Financial Memorandum, it was estimated

<sup>109</sup> For current information on the status of implementation, see [http://ec.europa.eu/justice/policies/privacy/lawreport/index\\_en.htm#firstreport](http://ec.europa.eu/justice/policies/privacy/lawreport/index_en.htm#firstreport) (Accessed on 5/11/2015)

<sup>110</sup> [2002] EWCA Civ 1373, [2003] QB 633 at [96].

<sup>111</sup> Joined Cases C-465/00, C-138/01, and C-139/01 [2003] ECR I-4989



that compliance with the then transitional regime would result in start-up costs to private sector data-users of some £836 million, with recurring costs of £630 million. The start-up costs for the public and voluntary sectors were estimated at £194 million and £120 million respectively, with recurring costs of £75 million and £37 million. These figures are in addition to the costs incurred in complying with the 1984 data protection regime, although no evidence has been published as to the scale of the present costs. The Home Office Regulatory Appraisal and Compliance Cost Assessment makes it clear that estimates are based upon a very small sample of users. Only four large and three small manufacturers were surveyed, for example, and although much publicity has been given to headline figures of £1 billion cost arising from implementation, the assessment document itself highlights the need to approach these estimates with caution. The Commissioner has also questioned the accuracy of the financial calculations,<sup>112</sup> suggesting that this may have resulted from misunderstandings as to the nature of the Data Protection Directive's requirements. To justify costs of some £20 for every inhabitant of the United Kingdom, it is to be hoped that the new legislation—perhaps coupled with other legislative initiatives in the field of human rights and freedom of information—will provide the basis for enhanced public awareness of the crucial importance of information in modern society, and the need to secure an appropriate balance between those who hold and use data and those who may be affected by such activities.

#### **VII. The African Union Data Protection Convention 2014:**

The potentially most important development in data protection regulation and policy in Africa is the adoption on 27 June 2014 of the African Union Convention on Cyber-security and Personal Data Protection,<sup>113</sup> at the African Union's Summit in Malabo, Equatorial Guinea. The African Union (AU), which has as its members all 54 African states except Morocco, was developing since 2011, a draft Cyber-security Convention (now renamed to include data protection). Inclusion of Chapter II of the Convention, 'Personal Data Protection', means that State parties who accede to and ratify the Convention are committed

---

<sup>112</sup>Press Release, 28 January 1998

<sup>113</sup> See <https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/african-union-convention-cyber-security-and-personal-data-protection-0> (Accessed on 5/11/2015)





to ‘establishing a legal framework’ based on its provisions, although this is stated to be ‘without prejudice to the free flow of personal data’.<sup>114</sup> Africa is now the first Continent outside Europe to adopt a data protection Convention.

The starting points are conventional EU-influence definitions of ‘personal data’ in terms of direct or indirect identifiability of a person, of ‘processing’ in broad terms, and of a ‘data controller’.<sup>115</sup> Its scope extends to the public and private sectors generally, and to automated and non-automated processing.<sup>116</sup> Processing relating to ‘public security, defense, research, criminal prosecution or State security’ is covered but allowed to be subject to some exceptions defined by specific provisions in existing laws. Processing exclusively for an individual’s ‘personal or household activities’ is exempt, but not where ‘for systematic communication to third parties or for dissemination’. Any processing for journalistic or research purposes is exempt, if conducted within professional codes of conduct, as well as any processing for artistic or literary expression<sup>117</sup>.

---

<sup>114</sup> Article 8 on the African Union Convention on Cyber-security and Personal Data Protection,

<sup>115</sup> Article 1 on the African Union Convention on Cyber-security and Personal Data Protection.

<sup>116</sup> Article 9 of the African Union Convention on Cyber-security and Personal Data Protection.

<sup>117</sup> Article 14.3 of the African Union Convention on Cyber-security and Personal Data Protection.



**CHAPTER THREE: DATA PROTECTION PRINCIPLES DERIVED FROM THE EUROPEAN UNION AND THEIR APPLICATION ON CLOUD-BASED TECHNOLOGIES:**

**1. Identifying personal data in the European Data Protection Regime:**

**1. Personal data**

The Data Protection Directive defines personal data in relatively simple terms as ‘any information relating to an identified or identifiable natural person (data subject)’.<sup>118</sup> The United Kingdom’s 1998 Data Protection Act’s approach is rather more complicated and analysis needs to proceed through a number of steps. The legislation initially states that it applies to ‘data which, relate to a living individual’.<sup>119</sup> The Act contains a further addition, providing that the term extends ‘to any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual’.<sup>120</sup> This represents in large part an unfortunate legacy from the original Act of 1984 which included a widely criticized distinction between statements of opinion( which were classed as personal data)and statements of the data controller’s intentions towards the data subject(which were not). The argument put forward by the government of the day was that statements of intention were personal to the data controller rather than to the subject. This is certainly arguable, but the point applies with equal if not greater validity with regard to statements of opinion. Even the then Data Protection Registrar was moved to comment to the effect that he found the distinction unclear and the provision in the Data Protection Act 1998 should perhaps be seen as a measure to remove what had generally been considered an unsatisfactory distinction, rather than a deliberate effort to depart from the requirements of the Directive.<sup>121</sup> There are, however, significant questions whether the Act’s provisions fully meet the requirements of the Directive. The threat of legal action by the European Commission alleging a failure properly to implement the Directive has been looming for a number of years. One perhaps peripheral issue is whether the legislation should apply to data relating to deceased individuals. The Directive, it will be

<sup>118</sup> Article 2(a) of the European Union’s Data Protection Directive.

<sup>119</sup> Section 1(1) of the United Kingdom’s Data Protection Act 1998

<sup>120</sup> Lloyd J. Ian, *Information Technology Law, Sixth Edition* p.40

<sup>121</sup> Lloyd, *Information Technology Law, Sixth Edition* p.40



recalled, applies in respect of data relating to a 'natural person'. It is arguable that this state continues after the individual's death. A minority of Member States have, indeed, chosen to extend their national laws to this category of data. Even accepting the validity of the United Kingdom's interpretation of the concept of a 'natural person' as a living individual, there may be circumstances in which data concerning a deceased person may also have implications for living individuals and therefore come within the scope of the legislation. Certain diseases such as haemophilia are hereditary in nature. The son of a woman suffering from the disease in its active form will always inherit the condition. Data indicating the mother's condition will therefore convey information about the medical condition of any male children. Again, some EU Member States apply at least elements of the legislation to data relating to legal persons. The United Kingdom does not, although it should be noted that legal persons do acquire some protection under the provisions of the communications-specific Directive on universal service and users' rights relating to electronic communications networks and services.<sup>122</sup> Although in its early stages data protection law tended to apply almost exclusively to textual information, developments in technology mean that almost any form of recorded information is likely to come within the ambit of the legislation. In the event that an individual interacts with an automated telephone service by speaking a series of numbers or words to allow a call to be directed to the appropriate department, those recorded words will class as personal data. Again, CCTV or similar camera systems generally fall within the scope of the legislation in respect of the video images recorded.<sup>123</sup>

Much attention is paid today to the collection and use of biometric data in situations such as the issuance of passports and visas. Although the term does not have a precise definition, it is generally regarded as encompassing two categories of data. The first relates to the physiological characteristic relating to aspects of physical identity. This category would include items such as fingerprints and, perhaps relating to more advanced forms of technology, face and iris recognition. A second category of biometric data relates to what are referred to as behavioural characteristics. As the name suggests, this concerns the manner in which a person acts. A simple and long-established example would relate to the manner in which a person signs his or her

<sup>122</sup> Directive 2009/136/EC, OJ 2009 I, 337/11.

<sup>123</sup> Lloyd, *Information Technology Law*, Sixth Edition p.40



name. More technologically advanced versions relate to the use of software to monitor the manner in which a particular individual uses a computer keyboard in terms of the speed, accuracy, and force with which keys are depressed. Biometric data, which forms a cornerstone of modern passports, is clearly an aspect of personal data. Data may be objective or subjective and, indeed, true or false. In an Opinion on the concept of personal data,<sup>124</sup> the Article 29 Working Party suggested that:

*As a result of a neuropsychiatric test conducted on a girl in the context of a court proceeding about her custody, a drawing made by her representing her family is submitted. The drawing provides information about the girl's mood and what she feels about different members of her family. As such, it could be considered as being 'personal data'. The drawing will indeed reveal information relating to the child (her state of health from a psychiatric point of view) and also about e.g. her father's or mother's behaviour. As a result, the parents in that case may be able to exert their right of access on this specific piece of information.*

As indicated in the above example, personal data may relate to more than one person, a topic which will be exploited in this chapter.

## **2. Sensitive data**

Any piece of information, however insignificant, might be classed as personal data. The extent to which certain forms of data can be classed as especially sensitive and deserving of special protection has long been a contentious issue. During the passage of the United Kingdom's Data Protection Act 1984, the attempt to identify sensitive data was considered a fool's errand by the English Parliament. In the case of personal data, the context in which data was held or used was considered far more important than the data itself. A list of names and addresses, for example, would not normally be considered sensitive, but this view might change if it referred to the movements of prominent persons and was in the hands of a terrorist organisation. Whilst this view is not without merit, it does seek to transform the exceptional into the norm. Almost invariably, however, data protection statutes have recognised that there are certain categories of information which would generally be regarded as possessing a degree of sensitivity and the

<sup>124</sup> Available from [http://ec.europa.eu/justice\\_home/fsj/privacy/docs/wpdocs/2007/wp136\\_en.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf) (Accessed on 6/11/2015)



processing of which should be subjected to more stringent controls than would generally be applicable. The Data Protection Act provides for special treatment for data relating to: the racial or ethnic origin of the data subject; his political opinions; his religious beliefs or other beliefs of a similar nature; whether he is a member of a trade union; his physical or mental health or condition; his sexual life; the commission or alleged commission by him of any offence; or any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings, or the sentence of the court in such proceedings.<sup>125</sup> With the exception of substituting the term ‘other beliefs of a similar nature’ for the Directive’s ‘philosophical beliefs’, the Act’s terminology mirrors that of the Directive.

In addition to covering a wide range of categories of information, the scope of particular categories has been broadly interpreted by the courts. In *Bodil Lindqvist*<sup>126</sup> the European Court of Justice was asked to give a preliminary ruling in response to a number of questions posed by the Swedish courts. Mrs. Lindqvist had been convicted of breaches of the Swedish data protection law in respect of her work as a catechist in the Swedish Lutheran Church and preparation of a number of WWW pages which contained information about Mrs. Lindqvist and eighteen of her parish colleagues, including brief details of the nature of their work and hobbies. It appears that much of the information was presented in what was intended to be a light-hearted manner. One particular item of information which was the cause of specific investigation was the indication that a named person had injured her foot and as a consequence was able to work only on a part-time basis. The essential question posed to the Court was whether such data constituted sensitive information regarding that person’s medical health, as such Mrs. Lindqvist was prosecuted by the Swedish authorities on a number of charges, including one of processing sensitive personal data without having secured authorization from the data protection authorities. The court’s reply was succinct and emphatic:

---

<sup>125</sup> Section 2 of the United Kingdom’s Data Protection Act.

<sup>126</sup> Case 101/01, [2004] QB 1014.



*In the light of the purpose of the Directive, the expression data concerning health used in Article 8(1) thereof must be given a wide interpretation so as to include information concerning all aspects, both physical and mental, of the health of an individual.*<sup>127</sup>

In some respects, the decision in *Bodil Lindqvist* illustrates the difficulties surrounding the concept of sensitive data. Once included in a list of sensitive data, it is almost impossible to say that a reference to illness or injury is not included, but as indicated above context is perhaps more important than content. A reference to the fact that an athlete was unable to compete in a race because of a broken leg, for example, does not seem to be possessed of a sufficient degree of sensitivity to justify the imposition of additional controls.<sup>128</sup>

I. Relating to the data subject

In *Bodil Lindqvist*, there was no doubt that the information about the foot injury related to the individual concerned. In other cases the situation may be more complex. In the example of the child's drawing cited above, the data contained might relate in varying degrees to the child and to other family members. Neither the Directive nor the Act provides any definition when data relates to an individual and this has been a rather contentious issue. The point was discussed extensively in the case of *Durant v Financial Services Authority*<sup>129</sup> and more recently has been considered in an Opinion of the Article 29 Working Party and in Guidance produced by the United Kingdom's Information Commissioner together with the decision of the House of Lords in the case of *Scottish Information Commissioner v Common Services Agency*.<sup>130</sup> In *Durant*, the appellant had been involved in a protracted dispute with Barclays Bank. This had resulted in unsuccessful litigation in 1993 and a continuing course of complaints to the industry regulatory body, the Financial Services Authority (FSA). The present case arose from a request from the appellant for access to a range of records under the ambit of the subject access provisions of the Data Protection Act 1998. Although some information was supplied, access to other records was

---

<sup>127</sup>Case 101/01, [2004] QB 1014

<sup>128</sup>Case 101/01, [2004] QB 1014

<sup>129</sup>*Durant v Financial Services Authority* [2003] EWCA Civ 1746.

<sup>130</sup>*Scottish Information Commissioner v Common Services Agency*[2008] UKHL 47.



provided only in partial form through the concealment or redaction of information which it was considered related to third parties.<sup>131</sup> Other records were withheld on the grounds either that the information contained therein did not constitute personal data relating to the appellant, or in the case of a number of records which were maintained in manual filing systems, that the system was not covered by the Data Protection Act. Although there was no doubt that much, if not all, of the data in question had been generated following complaints from the appellant, the critical issue was whether it related to him. Counsel for Durant argued that the term '*relate to*' should be interpreted broadly to encompass any data which might be generated following a search of a database made by reference to an individual's name. Thus, for example, a document describing the action which had been taken in response to a complaint from the appellant would be classed as personal data by virtue merely of the fact that his name would appear within the text. Counsel for the respondent advocated a more restrictive approach, making reference to the Shorter Oxford English Dictionary, which contained two definitions of the term, a broad reference to having '*some connection with, be connected to*' and a more restrictive notion that there should be reference to or concern with a subject, '*implying, in this context, a more or less direct connection with an individual*'. This more restrictive interpretation was adopted by the Court of Appeal. The purpose of the subject access provisions in the legislation was, it was stated, to enable the data subject to verify that processing did not infringe his or her rights of privacy and to exercise any available remedies in the event this was considered not to be the case. The purpose of the legislation was not, it was held, to give an automatic right of access to information purely by virtue of the fact that he might be named in a record or have some interest in the matters covered. In particular, it was stated, subject access was not intended to assist him, for example, to obtain discovery of documents that may assist him in litigation or complaints against third parties. Giving effect to this principle was that the mere fact that a search of a computer's contents by reference to a data subject's name revealed a number of documents did not mean that these documents necessarily constituted personal data relating to the subject. A more sophisticated analysis was required, The Court thus opined that:

---

<sup>131</sup>Lloyd, *Information Technology Law, Sixth Edition* p.40



*... there are two notions that may be of assistance. The first is whether the information is biographical in a significant sense, that is, going beyond the recording of the putative data subject's involvement in a matter or an event that has no personal connotations, a life event in respect of which his privacy could not be said to be compromised. The second is one of focus. The information should have the putative data subject as its focus rather than some other person with whom he may have been involved or some transaction or event in which he may have figured or have had an interest, for example, as in this case, an investigation into some other person's or body's conduct that he may have instigated. In short, it is information that affects his privacy, whether in his personal or family life, business or professional capacity.<sup>132</sup>*

This approach adopts, it is suggested, an overly restrictive view of the rationale of data protection laws. Whilst determining the legality of data processing and correcting errors certainly constitute important elements, equally important is the ability to become aware of what data is held. Much of the Data Protection Directive<sup>133</sup> and the Data Protection Act 1998's requirements relating to the factors legitimising data processing stress the importance of the data subject being aware of what is happening with regard to personal data. As was stated by the German Constitutional Court in the 1980s:

*The possibilities of inspection and of gaining influence have increased to a degree hitherto unknown and may influence the individual's behaviour by the psychological pressure exerted by public interest . . . if someone cannot predict with sufficient certainty which information about himself in certain areas is known to his social milieu, and cannot estimate sufficiently the knowledge of parties to whom communication may possibly be made, he is crucially inhibited in his freedom to plan or to decide freely and without being subject to any pressure/influence.<sup>134</sup>*

These factors support the adoption of an expansive definition of the scope of personal data. In a case such as *Durant*, it may well be that personal data in the form of an individual's name or other identifying data makes a peripheral appearance in a record. Rather than arguing that the appearance of the data does not come within the scope of the Act, it might be preferable to focus

---

<sup>132</sup> *Durant v Financial Services Authority* [2003] EWCA Civ 1746 at paras 27–28.

<sup>133</sup> Directive 95/46/EC.

<sup>134</sup> 'The Census Decision', *Human Rights Law Journal* 5 (1984), 94.





upon the extent of the information which might be supplied.<sup>135</sup> Whilst the court was clearly concerned that the data protection legislation was being invoked in the present case in the attempt to obtain discovery of documents and data that could not be obtained through other legal channels, it might have been preferable to have laid greater stress on the limited nature of the information which would be classed as personal data. The Information Commissioner has subsequently noted that ‘the Court of Appeal was widely understood to have adopted a rather narrower interpretation of personal data . . . than most practitioners and experts had followed previously’.<sup>136</sup> The Article 29 Working Party’s Opinion provides extensive guidance when data relates to an individual. Referring to its previous work in relation to RFID chip technology, it affirms that ‘*data relates to an individual if it refers to the identity, characteristics or behaviour of an individual or if such information is used to determine or influence the way in which that person is treated or evaluated*’.<sup>137</sup> The Opinion identifies three elements which may indicate that data relates to a particular individual. These are referred to as *content, purpose, and result elements*. The distinction between the elements may be complex on occasion but the Working Party stress that only one element needs to be present in order to justify a finding that data relates to a particular individual. The content element will be satisfied when information is about an individual. A medical or personnel record, for example, will fall within this category. The purpose element applies when the data is intended to be used to determine the manner in which an individual is treated. Data may, for example, be recorded by an employer of the websites accessed from workplace computers. The purpose may be to take disciplinary action against employees who violate Internet usage policies. Finally, a result element applies when the use of data, even though not collected originally for that purpose, is likely to have even a minor impact upon an individual’s rights and interests. Guidance produced by the United Kingdom’s Information Commissioner emphasizes similar criteria, suggesting that:

---

<sup>135</sup>Lloyd, *Information Technology Law, Sixth Edition* p.40

<sup>136</sup>Data Protection Technical Guidance, ‘*Determining what is personal data*’, p.6

<sup>137</sup>Working Party Document No. WP 105: ‘*Working document on data protection issues related to RFID technology*’, adopted on 19 January 2005, p. 8.



*Data which identifies an individual, even without a name associated with it, may be personal data where it is processed to learn or record something about that individual, or where the processing of that information has an impact upon that individual.*<sup>138</sup>

The most recent development in the field has come with the decision of the House of Lords in the case of *Common Services Agency v Scottish Information Commissioner*.<sup>139</sup> The case revolved around what is a complex and sometime difficult relationship between two statutes that are concerned with rather different aspects of information policy. This case was concerned with a request submitted to the appellant agency, a Health Board, under the terms of the Freedom of Information (Scotland) Act 2002<sup>140</sup> for the provision of information relating to instances of childhood cancer within the locality of a nuclear power station. Under the terms of the 2002 Act a range of exceptions apply regarding the types of information which may be supplied and, in particular, it is stated that personal data is not to be disclosed where this would be in contravention of any of the data protection principles.<sup>141</sup> Relying on this provision the appellant refused to disclose information. The Scottish Information Commissioner ruled that such a blanket refusal was unlawful. Although the raw data identifying individual patients was undoubtedly personal data disclosure would not be in breach of the data protection principles were to it be processed using a procedure known as 'barnardisation' which would modify statistical elements so that no individual could be identified. The appellant was ordered to conduct such a process. The Commissioner's ruling was upheld by the highest Scottish court, the Court of Session.<sup>142</sup> Applying the approach of the Court of Appeal in *Durant v Financial Services Authority*<sup>143</sup> that '*mere mention of the data subject in a document held by a data controller does not necessarily amount to personal data*'<sup>144</sup> the Lord President ruled that:

---

<sup>138</sup> Working Party Document No. WP 105: 'Working document on data protection issues related to RFID technology', adopted on 19 January 2005, p. 8.

<sup>139</sup> *Common Services Agency v Scottish Information Commissioner* [2008] UKHL 47.

<sup>140</sup> According to Ian J Lloyd, The Scottish legislation is equivalent in all relevant respects to the Freedom of Information Act 2000 applying in England and Wales

<sup>141</sup> Section 38

<sup>142</sup> [2006] CSIH 58

<sup>143</sup> [2003] EWCA Civ 1746

<sup>144</sup> [2003] EWCA Civ 1746 At para. 28.



*Although the underlying information concerns important biographical events of the children involved, by the stage of the compilation of the barnardised table that information has become not only statistical but perturbed to minimise the risk of identification of any individual child. It is no longer, in respect of any child, 'biographical in a significant sense'. The focus has, in my view, also moved away from the individual children to the incidence of disease in particular wards in particular years. The rights to privacy of the individual children are not infringed by the disclosure of the barnardised data.<sup>145</sup>*

A further appeal was made to the House of Lords where, delivering the leading judgment, Lord Hope gave detailed consideration to the scope of the definition of personal data and also of sensitive personal data. In respect of the former he indicated that the Court of Appeal decision in *Durant* should be distinguished as it related to the operation of the subject information provisions rather than the definition of personal data per se. The answer to that issue, he held, 'must be found in the wording of action 1(1) (of the Data Protection Act 1998) read in the light of Council Directive 95/46/ EC.'<sup>146</sup> The Act refers to the possibility that an individual might be identified from data 'and other information which is in the possession of the data controller'. As the appellant had the means to recreate data identifying individuals, the barnardised data remained personal data. Turning to the question whether the data could be disclosed in conformity with the provisions of the Act, Lord Hope cited the provisions of Recital 26 of the Directive to the effect that when data was truly anonymous 'the principles of protection shall not apply to data'. Section 1(1) it was held, gave effect to this provision. As noted previously, Recital 26 of the Directive states that in making decisions as to whether an individual can be identified 'account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person'.<sup>147</sup> The appellant clearly had the means to match data to named individuals but the issue in this respect was whether a third party receiving the barnardised data would be able to re-engineer it. The Scottish Information Commissioner, it was held, should have considered more fully this issue and, accordingly, the case was remitted for him to make

<sup>145</sup>[2003] EWCA Civ 1746 , At para.23

<sup>146</sup>[2003] EWCA Civ 1746, At para 20.

<sup>147</sup> Lloyd J. Ian, *Information Technology Law*, p. 43



findings of fact in this respect. Ultimately, the Commissioner issued a further ruling<sup>148</sup> holding that he was not satisfied that anonymity could be guaranteed and on this basis the freedom of access request was denied. In some respects the decision in Common Services Agency might be seen to have limited the application of the Court of Appeal case in Durant although the rather opaque way in which it has been done cannot eliminate all scope for confusion. What appears to be the effect of Lord Hope's dicta is that any element of data relating to an individual will be classed as personal data.

## **II. Issues of identification.**

The premise underlying data protection legislation is that the processing of data relating to individuals constitutes a threat to the subject's rights and freedoms. If an individual cannot be identified from the manner in which data is collected, processed, or used, there can be no significant threat to privacy and no justification for the application of legislative controls. The Data Protection Directive provides that: an identifiable person is one who can be identified directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, psychological, mental, economic, cultural or social identity.<sup>149</sup> Also relevant are the provisions of Recital 26 to the Directive. This states that:

*Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person.*

The United Kingdom's Data Protection Act 1998 provides that personal data: . . . *means data which relates to a living individual who can be identified— (a) from those data; or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller.*

---

<sup>148</sup> Available from <http://www.itspublicknowledge.info/applicationsanddecisions/Decisions/2005/200500298.asp> (Accessed on 11/6/2015)

<sup>149</sup> Directive 95/46/EC, Article 2(a).



It will be recognised that the Directive and the Act differ in that the Act restricts its application to information which is or is likely to come into the possession of the data controller. The Directive's application is open-ended, applying whenever anyone might be able to identify an individual. A recent example might illustrate a difference between the two approaches. In 2006, AOL placed on the Internet data relating to search requests made by millions of its subscribers. Although no names were published, in at least some cases it proved possible to identify individuals following analysis of their search history. One case concerned a user allocated the identifying number 4417749. This user had conducted searches on a range of topics, including medical conditions relating to humans and animals, landscape gardening, persons with a particular surname (Arnold), and house sales in a particular area of the United States. Taking this data, researchers focused on a particular individual, Thelma Arnold, who, when read in a list of the searches, confirmed that they had been made by her.<sup>150</sup>

Under the United Kingdom approach, it is likely that the data would not have been considered personal data at the point it was compiled by AOL because that organisation would not have possessed the necessary additional information to identify users.<sup>151</sup> Under the Directive's criteria, the material would probably have been classed as personal data, as AOL would have been required to consider the possibility that third parties could perform the task of identification. It is likely that if its disclosure and decoding were to be carried out in the United Kingdom (or any other state of the European Economic Area (EEA)) the person identifying individuals would be classed as a data controller in his or her own right and subject to the same obligations to comply with data protection law. Matters would be much less satisfactory were the decoder to be located outside of the EEA and, of course, dissemination of information via the Internet is global in its nature. The AOL example undoubtedly represents an extreme case but the issue of identifiability may frequently be an issue. Once again, the Article 29 Opinion on the concept of personal data identifies a wide range of potential situations and provides extensive guidance. Linking data to a

---

<sup>150</sup><http://www.iht.com/articles/2006/08/09/business/aol.php> (Accessed on 11/06/2015)

<sup>151</sup> Given that AOL operates on a subscription service it may be that the company would have possessed the necessary data. The example might be more accurate in the event that it applied to an organisation such as Google, which does not require users to give their names. Indeed, one of the reasons why Google refused to comply with a United States government request for access to search data was because of concerns that individuals might be identified. See <http://news.bbc.co.uk/1/hi/technology/4630694.stm> (Accessed on 11/06/2015)



upon request. Prior to the introduction of these regulations, the officers were required to supply copies of the Register only where these were readily available. The consequence was a massive increase in the usage of data from the Electoral Rolls for direct marketing and similar purposes. Following the report of a working group, the Home Secretary reported to Parliament concerns that:

*As the law stands, anyone may buy a copy of the electoral register for any purpose. The Home Office and electoral administrators receive more complaints about that than any other subject. People are unhappy about the large amount of unsolicited mail (junk mail) from companies that have obtained their details from the electoral register. Perhaps more worryingly, the advent of powerful CD-ROMs compiled from the electoral register, which allow for searching by name, means for example that abusive spouses can trace their former partners with considerable ease using a single CD-ROM. People who feel threatened in that way may simply not dare to register. All of that, together with the requirements of the European Union data protection directive,<sup>184</sup> which was signed and agreed by the previous Administration and, generally, of the right to privacy, led the working party to conclude that it was wrong that people should be under a statutory obligation to provide their details for electoral registration purposes and then have no say about whether that information could be used for other unrelated purposes.<sup>185</sup>*

Section 9 of the Representation of the People Act 2000 made provision for regulations to be made to establish two versions of the Electoral Register. As implemented in the Representation of the People (England and Wales) (Amendment) Regulations 2002,<sup>20</sup> voters will be given information regarding the purposes for which data contained in the register might be used and given the opportunity to opt out of having their data disclosed. Registration officers will then be charged with producing two registers. The full register will contain details of all persons eligible to vote, which will be restricted to electoral purposes and a number of closely defined applications. Although this is available for public consultation it is provided in Regulation 6 that:

---

<sup>184</sup> Directive 95/46/EC.

<sup>185</sup> 357 HC Official Report (6th series), col. 168, 30 November 1999.



*A person who inspects the full register and makes a copy of it or records any particulars included in it otherwise than by means of hand-written notes shall be guilty of an offence.*

An edited copy excluding the details of those who have opted out will also be produced, which may be supplied and used for commercial purposes.<sup>186</sup> By 2005, around 30 per cent of voters had exercised their right to opt out of the commercially available Electoral Register. Such a level would diminish the value of the resource. The data held on the B4U.com website was taken from the 2001 Electoral Roll, the last created before the 2002 Regulations. The use to which the data was put was lawful under the law as it stood at the time that the Electoral Roll was drawn up. However, the Information Commissioner determined that the use of the data in 2006 constituted unfair processing. The Commissioner through the enforcement notice asserted that he considered that it is inherently unfair for individuals to be compelled to provide personal information on penalty of a criminal conviction only for that information to be subsequently disclosed to commercial organisations without any express restrictions on its use. The Commissioner went on to state that, given that individuals had been given a right to request that they are excluded from the edited register, it was rather unfair to undermine the express wishes of those who have exercised that right and the 2002 Regulations by continuing to make the relevant data available on the data controller's website. Moreover, the Commissioner considered that the processing of the relevant data by the data controller is unfair given that a significant proportion of the individuals whose details are contained in the relevant data will have subsequently exercised their right not to have those details included in the edited electoral register. Accordingly, the website owner was ordered to cease making the data available on its website.<sup>187</sup>

The case can perhaps be seen as a borderline one and it is perhaps unfortunate that the Information Tribunal was not called upon to deliver a determination. If data was 10-years old, could processing still be classed as unfair? Or 20-years old? Data controllers should be able to assess whether their processing will comply with the requirements of the legislation and at least in this area, it is submitted, the state of the law is insufficiently precise. Although Electoral

---

<sup>186</sup> Section 9 of the Representation of People's Act (2000)

<sup>187</sup> Currently, the B4U.com site holds no evidence of having such data, however a sister site does exist that sells 'electrical goods'. [http://www. B4U.com](http://www.B4U.com) (Accessed on 7/11/2015)



Registers may represent the most extensive record of their kind, similar issues have arisen with other forms of records which are required to be made available to the public. Concern has been expressed on a number of occasions at the use made of lists of company shareholders, particularly in the case of privatised undertakings which might have several hundred-thousand shareholders. It may be argued that the purpose of making details of shareholders publicly available is to allow identification of the owners of a limited liability company. Use of this information for the purposes of compiling mailing lists for direct marketing purposes raises different issues, although it is difficult to see how prohibitions might be enforced against the use of publicly available information for such purposes.<sup>188</sup>

One of the most recent cases concerned with the issue of fair processing is *Johnson v Medical Defence Union*.<sup>189</sup> The case centred upon whether the use of a risk assessment policy by the Medical Defence Union could be considered unfair. The scheme took account of the volume of incidents reported involving a particular member and it was an integral element that limited regard was taken of the outcome of such cases. The view was taken that if a doctor had a significant history of complaints brought against him in the past, this would be a reliable indicator that the trend would continue, and regardless of whether the previous complaints had proved to be unfounded. The prediction would be that the Medical Defence Union would be required to incur continuing expenditure in representing the doctor in the future. Although there was disagreement between the judges on whether processing had taken place, there was unanimity on the issue of fairness. At trial, having taken account of the decision of the Data Protection Tribunal in the case of *CCN Systems v Data Protection Registrar*,<sup>190</sup>, Mr. Justice Rimer concluded that:

*.. "There is in principle nothing relevantly unfair about the MDU's risk assessment policy or about the way in which it processed information in applying that policy. . . . The policy is directed at risk management (preserving the MDU funds against a risk of claims, and the*

---

<sup>188</sup> In the recent conversion process of the Halifax Building Society, members were encouraged to place their new shareholding in a nominee account administered by the Society. One advantage claimed for this was that the shareholder's name and address would not appear on publicly available registers.

<sup>189</sup> *Johnson v Medical Defence Union*. [2007] EWCA Civ 262.

<sup>190</sup> *CCN Systems v Data Protection Registrar*, Available from

[http://www.informationtribunal.gov.uk/Documents/decisions/cnn\\_systems.pdf](http://www.informationtribunal.gov.uk/Documents/decisions/cnn_systems.pdf) (Accessed on 7/11/2015)





*incurring of costs, in the future. The MDU experience is that a risk of that nature cannot be measured simply by awaiting the happening of a statistically significant number of occurrences that do in fact cause a drain on its funds.*<sup>191</sup>

The Court of Appeal upheld this position and pointed out that the MDU's risk assessment policy was fair in accordance with the first data protection principle and no actions undertaken by the Union had proved to the contrary.

## **II. Lawful Processing:**

As with the requirement of fairness, neither the Act nor the Directive provides any definition when conduct will be lawful. In the decision of the House of Lords in *R v R*, a case concerned with marital rape, the concept of unlawful conduct was defined by Lord Keith as relating to 'something which is contrary to some law or enactment or is done without lawful justification or excuse'.<sup>192</sup> In *Legal Guidance on the Act*,<sup>193</sup> the Information Commissioner indicated that it was necessary for a data controller to comply with all relevant rules of law whether derived from statute or common law, relating to the purpose and ways in which the data controller processes personal data.

A number of particular areas were identified as being of particular relevance, these included confidentiality arising from the relationship of the data controller with the data subject; the ultra vires rule and the rule relating to the excess of delegated powers, under which the data controller may only act within the limits of its legal powers; legitimate expectation, that is, the expectation of the individual as to how the data controller will use the information relating to him; and Article 8 of the European Convention on Human Rights, which demands the right to respect for private and family life, home, and correspondence.

It is essential to note that the concepts of lawfulness and fairness are largely intertwined and thusly, in the course of their application, do collide in numerous occasions.

---

<sup>191</sup> *CCN Systems v Data Protection Registrar*, [2006] EWHC 321 (Ch) at para. 122.

<sup>192</sup> *CCN Systems v Data Protection Registrar*, at para. 124

<sup>193</sup> Available from [http://www.ico.gov.uk/upload/documents/library/data\\_protection/detailed\\_specialist\\_guides/data\\_protection\\_act\\_legal\\_guidance.pdf](http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/data_protection_act_legal_guidance.pdf). (Accessed on 7/11/2015)



A. Consent and data:

Over the years, there has been extensive debate on how a data subject may validly give consent to the processing of personal data. Anyone who has entered into almost any form of mail order or online transaction will be familiar with the basic techniques which are used. Typically, as was described in the context of the *Innovations and Linguaphone* Tribunal cases discussed below, a note of the data controller's processing intentions will be given on an order form or similar document.

Under what is referred to as an 'opt-out' procedure, the data subject will be told that the specified forms of processing will take place unless notice of objection is received. This would normally require that the subject places a mark in an 'opt-out' box. The alternative approach, referred to as 'opting in', is again to give notice of the desired forms of processing but also to ask the data subject to indicate that they are content for this to take place. Typically, data controllers have sought to maximize the use of the former technique, as it is well accepted that this will maximise the number of persons whose data may be processed. In many cases, data subjects may not read the notice or may be unaware of the full implications of what is being proposed. A typical formulation might be along the lines, '*We would like to share your data with other carefully selected companies whose goods or services we consider may be of interest to you.*' Of course, the real implications of such consent would be the sale of the data to the highest bidder. Whilst data subject apathy may help controllers on an opt-out basis, the reverse will be the case where subjects are asked to opt in.

Schedule 2 to the United Kingdom's Data Protection Act 1998 provides that processing will be lawful when 'the data subject has given his consent to the processing'. Schedule 3 requires that the subject gives 'explicit consent'. Neither phrase is defined in the Act. The Data Protection Directive is a little more helpful, providing that the data subject's consent can be defined as any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.<sup>194</sup>

---

<sup>194</sup>Directive 95/46/EC, Article 2(h).



In the context of consent to the processing of data, the Directive requires that consent be given unambiguously. This term is not defined. As interpreted in the United Kingdom, it is generally seen as being compatible with either an opt-out or opt-in approach, with the basic requirement being that the data subject is able readily to give an indication of his wishes. Albeit in a different context, the Article 29 Working Party appears to suggest that an opt-in approach may be needed. In an ‘Opinion on unsolicited communications for marketing purposes’<sup>195</sup> it considered the requirement in the Privacy and Electronic Communications Directive that prior consent be obtained before commercial emails are sent to data subjects. It asserted that implied consent to receive such mails is not compatible with the definition of consent of Directive 95/46/EC and in particular with the requirement of consent being the indication of someone’s wishes, including where this would be done ‘unless opposition is made’ (opt-out). Similarly, pre-ticked boxes, e.g., on websites are not compatible with the definition of the Directive either. At least pending any court decision either in the United Kingdom or before the European Court of Justice, it appears that an ‘opt-out’ approach will be accepted in the United Kingdom. A key criteria in determining the acceptability of the technique concerns the clarity of the notification. In *Linguaphone Institute v Data Protection Registrar*,<sup>196</sup> a case brought before the Tribunal under the 1984 Act, the appellant included in its advertisements a notice to the effect that:

*(Please) tick here if you do not wish Linguaphone to make your details available to other companies who may wish to mail you offers of goods or services.*

In holding that there was a breach of the data protection principles, the Tribunal expressed concern that the opt-out box appeared in minute print at the bottom of the order form. In the Tribunal’s view the position, size of print and wording of the opt-out box did not amount to a sufficient indication that the company intended or wished to hold, use or disclose that personal data provided at the time of enquiry for the purpose of trading in personal data. Beyond giving

---

<sup>195</sup>Opinion 5/2004, available from [http://ec.europa.eu/justice\\_home/fsj/privacy/docs/wpdocs/2004/wp90\\_en.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp90_en.pdf) (Accessed on 7/11/2015)

<sup>196</sup>*Linguaphone Institute v Data Protection Registrar*, Case DA/94 31/49/1



information to the data subject, the controller must afford a reasonable opportunity for the subject to express consent (or the lack of it).<sup>197</sup>

This was at issue in another case brought before the Data Protection Tribunal under the 1984 Act, *Innovations v Data Protection Registrar*.<sup>198</sup> In this case, the appellant was in the business of mail order sales. Custom was solicited in a variety of ways, including the distribution of catalogues and the placing of advertisements in various media, including newspapers, radio, and television. The appellant's catalogues gave customers notice of this possibility and its order forms offered customers the opportunity to exclude use of their data for broking purposes. Some adverts, especially those appearing on radio or television, did not make mention of the possibility, and in the event that catalogue orders were placed by telephone, no mention would be made of this secondary purpose. An acknowledgement of an order would, however, be sent and this would convey the message:

*For your information. As a service to our customers we occasionally make our customer lists available to carefully screened companies whose products or services we feel may interest you. If you do not wish to receive such mailings please send an exact copy of your address label to . . .*

The Registrar took the view that notification of the intended use came too late in the contractual process and served an enforcement notice alleging a breach of the first data protection principle, which, as formulated under the 1984 Act, required that data be obtained fairly and lawfully. A number of arguments were put forward by the applicant as justifying their practices. It was suggested that, at the time of placing an order, customers would be concerned primarily with obtaining the goods and that a notice along the lines referred to above would have limited impact. Where orders were made by telephone, giving specific notice would increase the length of the call, thereby increasing costs for both the supplier and the customer. It was also pointed out that the details would not be used for list-broking purposes until thirty days from the date the acknowledgement order was sent. This, it was suggested, allowed ample time for the customer to opt out. It was also pointed out that the appellant's practices were in conformity with an industry code of practice and the Council of Europe's Recommendation on the protection of personal data

<sup>197</sup> Lloyd J. Ian, *Information Technology Law*, p. 93

<sup>198</sup> *Innovations (Mail Order) Ltd v Data Protection Registrar* Case DA/92 31/49/1.



used for the purposes of direct marketing.<sup>199</sup> Notwithstanding these factors, the Tribunal upheld the Registrar's ruling. Although codes of practice and recommendations might constitute useful guidance, the task for the Tribunal was to interpret the law. Use of the data for list-broking purposes, it was held, was not a purpose which would be obvious to the data subjects involved. Fair obtaining required that the subject be told of the non-obvious purpose before the data was obtained. Whilst a later notification might 'be a commendable way of providing a further warning', it could not stand by itself. Where prior notification might not be practicable, the Tribunal ruled that 'the obligation to obtain the data subject's positive consent for the non-obvious use of their data falls upon the data user'.<sup>200</sup>

An important aspect of the concept of consent in data protection regulation is its duration. Consent is not a permanent condition. It is open to a data subject to withdraw consent at any time. This point is not specified directly in either the Data Protection Act or the Directive. Article 9 of the Directive on Privacy and Electronic Communications,<sup>201</sup> which refers specifically to the processing of personal data in the electronic communications sector,<sup>202</sup> provides that users or subscribers shall be given the possibility to withdraw their consent for the processing of location data other than traffic data at any time. There is no doubt that whilst the withdrawal of consent cannot have retrospective effect, it would serve to render unlawful any future processing which is dependent upon this head of authority.<sup>203</sup>

### **3. Unlawful acquisition of personal data:**

The second data protection principle requires that personal data shall be obtained only for one or more specified and lawful purposes and shall not be processed further in any manner incompatible with that purpose or those purposes. Given the breadth of the definition of processing (which refers specifically to the obtaining of data) it is difficult to identify a real need for the second data protection principle. Indeed, much the same comment could be made regarding most of the remaining principles which refer to specific aspects of processing. In

---

<sup>199</sup> Recommendation 85/20

<sup>200</sup> *Innovations (Mail Order) Ltd v Data Protection Registrar* Case DA/92 31/49/1 at Para. 31.

<sup>201</sup> Directive 2002/58/EC, OJ 2002 L 201/37

<sup>202</sup> Directive 2002/58/EC, OJ 2002 L 201/37

<sup>203</sup> Lloyd J. Ian, *Information Technology Law*, p. 94



interpreting the second principle, the Act provides that the purposes for which data are to be processed may be specified either by the giving of notice to the data subject or in a notification given to the Commissioner. It is to be noted, however, that notification by itself will not satisfy the requirements of the first data protection principle. The more significant element of the second principle concerns what might be regarded as ongoing processing activities. Data may be obtained for one purpose with due notification given to the data subject but changes in circumstance or technical developments may make other forms of activity attractive to the controller.<sup>204</sup> The UK's Information Commissioner has indicated that a strict view will be taken in determining whether any future forms of processing whether carried out by the controller or by a third party to whom the data are disclosed are compatible with those originally notified to the Commissioner or to the data subject.<sup>205</sup> During recent years, considerable publicity has been attached to the activities of private investigators and investigative journalists, who, through various forms of subterfuge or bribery, were able to secure access to personal information held by a data user. Stella Rimington, the former head of MI5, for example, has been quoted as claiming that upon her appointment to MI5, The Sunday Times had employed a private investigator who had been able to discover where she lived, how much money she had in her bank account, the shops she regularly patronised, her (ex-directory) phone number, and the telephone numbers that she most frequently called<sup>206</sup>. In the situation where the investigator obtained direct access to data held on a computer, it would be likely that an offence would be committed under the United Kingdom's Computer Misuse Act 1990. In many instances, however, the information would be obtained, either through bribing an employee of the data user or by misleading the user as to identity and entitlement to access the data. In these situations, the investigator would not normally be guilty of any offence. To remedy this situation, section 55 of the Data Protection Act 1998 provides that an offence will be committed by a person who 'knowingly or recklessly, without the consent of the data controller' seeks to obtain or disclose personal data or procure its disclosure to a third party. An exception is provided where the data is obtained in connection with the prevention or detection of crime or in pursuance of a court order.

---

<sup>204</sup> Lloyd J. Ian, *Information Technology Law*, p. 95

<sup>205</sup> Legal Guidance, para. 3.2.

<sup>206</sup> Herald (formerly Glasgow Herald), 17 October 1996.



A further offence is committed by a person who sells or offers to sell data obtained in contravention of this provision. Both convictions are punishable by a fine of up to £5,000 in the Magistrates' Court and to a potentially unlimited amount in the Crown Court. In spite of the prohibition, there is extensive evidence that the trade in unlawfully acquired personal information is continuing at a rapid and unprecedented pace.<sup>207</sup>

#### **4. The principles of adequacy and relevance:**

The third data protection principle of the Data Protection Act 1998 asserts that data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed. The Data Protection Directive<sup>208</sup> uses the same term. No further guidance is available in either instrument concerning the application of these requirements.

The application of this data protection principles was at issue before the Information Tribunal in the case of *The Chief Constables of West Yorkshire, South Yorkshire and North Wales Police and the Information Commissioner*.<sup>209</sup> At issue in this case were the data retention practices of a number of police forces in respect of three individuals. In each case, the individual had been convicted of criminal offences: in one case, a single offence in 1979; in the second, five offences relating to the taking of motor vehicles, the last conviction also being in 1979; and in the case of the third data subject, five offences ending with a conviction for theft in 1969. In each case, the primary cause for complaint was that the information had been disclosed for purposes unconnected with the operation of the criminal record system: in one case, in connection with a complaint made by the data subject in respect of the conduct of a police officer; in another, to the United States immigration authorities in respect of a visa application; and in the third, in connection with an application for employment. Following the receipt of complaints from the data subjects, the Information Commissioner exercised his powers under section 42 of the Act to conduct an assessment of the legitimacy of the processing of the personal data. After extensive correspondence with the police authorities in question, the Commissioner served each with an

---

<sup>207</sup> Lloyd J. Ian., *Information and Technology Law*, p. 107

<sup>208</sup> Directive 95/46/EC.

<sup>209</sup> *The Chief Constables of West Yorkshire, South Yorkshire and North Wales Police and the Information Commissioner* Available from [http://www.informationtribunal.gov.uk/DBFiles/Decision/i204/north\\_wales\\_police.pdf](http://www.informationtribunal.gov.uk/DBFiles/Decision/i204/north_wales_police.pdf) (Accessed on 7/11/2015)



enforcement notice alleging breaches of the third and fifth data protection principles. The authorities appealed to the Information Tribunal. In all the cases, data had been retained on the police national computers and it was accepted that it was held in accordance with the latest version of 'Weeding Rules', which had been the subject of discussion, if not agreement, between the Information Commissioner (and his predecessors) and the Association of Chief Police Officers. In essence, these provide for details of relatively minor offences to be retained for 30 years and more serious offences for a period of 100 years, a period designed to ensure that the data is retained for the lifetime of the offender. It was accepted by the Tribunal that the Weeding Rules in their present form and edition demonstrated that there was some value in retaining conviction data dependent largely upon the nature of the offence. The Weeding Rules represent a considered exchange between the parties, i.e. the Commissioner on the one hand and ACPO on the other which has in the result forged some form of generalised understanding that after a given data, certain offences should be removed from the PNC(Police National Computer). However, the Tribunal found that the Weeding Rules do not and could not conceivably represent an unqualified and rigid code.<sup>210</sup> The Tribunal drew a distinction between retention and disclosure of the data. Accepting the benefit for policing purposes of retention of data, even at the level of maintaining links to fingerprint and DNA samples, it amended the Commissioner's ruling to require that within six months the appellants: . . . *procure that the Conviction Data relating to (the complainant data subjects) currently held on the PNC database be retained on the PNC subject to the retention rules of any current ACPO Code of Practice or any equivalent thereof and not be open to inspection other than by the data controller or by any other data controller who is or represents a chief officer of police.*<sup>211</sup>

The Commissioner returned to the question of the conformity of police data retention in the later case of *Chief Constable of Humberside Police and others v Information Commissioner*.<sup>212</sup> This marked the first occasion in which a decision of the Information Tribunal was the subject of an appeal to the Court of Appeal. The South Yorkshire case had focused in large part on issues

---

<sup>210</sup>*The Chief Constables of West Yorkshire, South Yorkshire and North Wales Police and the Information Commissioner* at Para. 206

<sup>211</sup>*The Chief Constables of West Yorkshire, South Yorkshire and North Wales Police and the Information Commissioner* .at Para 218

<sup>212</sup>*Chief Constable of Humberside Police and others v Information Commissioner*, [2009] EWCA Civ 1079.





concerned with the disclosure of data for purposes other than those concerned with core policing activities. These were again at issue in the Humberside litigation but attention was also given to the retention of data on the Police National Computer. Police Guidelines in England and Wales (a significant factor in the decision of the Tribunal was that Scotland operated a more subject-friendly policy) provided for the retention of almost all data relating to criminal convictions for a period of 100 years.<sup>213</sup>

Following a series of complaints from data subjects, the Commissioner served enforcement notices on five police forces, each relating to records relating to one individual and requiring removal of the data from the Police National Computer. As discussed in relation to the South Yorkshire case, access to data might be restricted although at issue in most of the present cases was an act of disclosure to other statutory agencies, generally in connection with the system of extended disclosure certificates introduced under the Police Act 1997.<sup>214</sup> Any person seeking to work with vulnerable individuals such as children is required to obtain such a certificate which will detail any criminal convictions or formal reprimands received by the individual. In four of the cases forming the basis of the enforcement notices the individuals concerned had been convicted of relatively minor criminal offences some time in the past. One subject, referred to as HP, had been convicted on two counts of shoplifting in 1984 when aged sixteen. No further convictions were recorded against him. The conviction details were listed on an enhanced disclosure certificate which he was required to obtain twenty-two years later when seeking a position with a local authority as a care officer. Three of the other cases were broadly similar but in the final case a 13-year old girl (referred to as SP) had been accused of assault. She had accepted a formal reprimand but was assured that details would be deleted from the Police National Computer when she reached the age of eighteen if she had not committed any further criminal offences. By the time of her eighteenth birthday, police policy had changed and the details were retained, again to appear on an enhanced disclosure certificate obtained in connection with an application for employment as a care worker. In this case the enforcement notice alleged also a breach of the first data protection principle that the retention of the data in breach of undertakings given constituted unfair processing. The Tribunal received statistical

<sup>213</sup> Lloyd J. Ian, *Information Technology Law*, p. 95

<sup>214</sup> *Chief Constable of Humberside Police and others v Information Commissioner*, at Para 23



evidence indicating that where individuals had such long periods without being convicted of any offences, the likelihood of them being convicted in the future was effectively the same as that of a person with no previous criminal conviction. The Tribunal agreed with the Commissioner that the continued presence of the data on the Police National Computer offered no significant operational benefits to the police and upheld the enforcement notice. It agreed also that the retention of data in the case of SP breached the first data protection principle. The police forces concerned appealed against the Tribunal decision and were successful before the Court of Appeal which was highly critical both of the Commissioner's original decision to serve the enforcement notices and of the Tribunal's decision to uphold them.

Delivering the leading judgment, Lord Justice Waller quoted the evidence given to the Bichard Enquiry. This was set up in the wake of a case in which a school caretaker had murdered two young girls. Subsequently evidence came to light that the caretaker was known to other police forces in connection with inappropriate conduct towards girls but that this information had not been passed on to the force in whose area the murders took place. Responding to suggestions by some police authorities that the requirements of data protection legislation had prevented the sharing of information, the then Information Commissioner gave evidence to the Inquiry which was summarised to the effect that, Police judgements about operational needs should not be lightly interfered with by the Information Commissioner. His office 'cannot and should not substitute their judgement for that of experienced practitioners'. His office should give considerable latitude to the police in their decision making. If a reasonable and rational basis exists for a decision, 'that should be the end of the story'.<sup>215</sup> The same principle, Lord Justice Waller held, should apply in the present case, 'If the police say rationally and reasonably that convictions, however old or minor, have a value in the work they do that should, in effect, be the end of the matter' It should be noted that the case of SP did cast a rift of opinion between numerous Honorable Judges of the Court, however the majority agreed that the processing had not been particularly unfair, as it was due to a change in policing policy and was not specifically directed at the plaintiff.

---

<sup>215</sup>*Chief Constable of Humberside Police and others v Information Commissioner* , At para. 4.45.2



### **5. Accuracy and Timeousness:**

The fourth data protection principle requires that: 'personal data shall be accurate and, where necessary, kept up to date'. Data is regarded as being inaccurate when it is 'incorrect or misleading as to any matter of fact'.<sup>216</sup> In the event that personal data is inaccurate, a data subject may be entitled to seek its rectification and, in certain cases, compensation for any resultant damage or distress.<sup>217</sup> The Data Protection Directive explains it as follows:

*The fourth principle is not to be regarded as being contravened by reason of any inaccuracy in personal data which accurately record information obtained by the data controller from the data subject or a third party in a case where— (a) having regard to the purpose or purposes for which the data were obtained and further processed, the data controller has taken reasonable steps to ensure the accuracy of the data; and (b) if the data subject has notified the data controller of the data subject's view that the data are inaccurate, the data indicate that fact.*<sup>218</sup>

These requirements are cumulative.

The second element of this principle requires that necessary updating of information shall be carried out. The question of whether updating is required will be dependent upon the nature of the data and the purpose to which it will be put. If the data is merely a record of a transaction between the data user and the data subject, no updating would be either necessary or justified. Where the information is being used as the basis for continuing decisions and actions, regular updating may be essential. Thus, where information is to be used for assessing an employee's suitability for promotion, an indication of periods of absence would require to be supplemented by any explanations which might subsequently have been provided.

### **6. Data Security:**

Under the terms of the United Kingdom's Data Protection Act 1998; data controllers and the operators of computer bureaux are obliged to ensure that appropriate technical and organisational

---

<sup>216</sup> Section 70(2), Data Protection Act 1998.

<sup>217</sup> Sections. 13–14, Data Protection Act 1998.

<sup>218</sup>, Article 6(1)(e), Directive 95/46/EC, Article 6(1)(e).



measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. Additionally, controllers will be responsible for ensuring that any data processors contracted by them comply with the requirements of the principle. The comparable requirement in the Data Protection Directive is that, *taking account of the state of the art and making an assessment of costs and risks involved: . . . the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network.*<sup>219</sup>

---

<sup>219</sup> Directive 95/46/EC, Article 17(1).



**CHAPTER FOUR: ANALYSING THE PRESENT DATA PROTECTION FRAMEWORK WITHIN THE KENYAN JURISDICTION THROUGH THE CONSTITUTION, KENYAN JURISPRUDENCE AND THE AFRICAN UNION'S CONVENTION ON PERSONAL DATA PROTECTION AND CYBERSECURITY:**

**Introduction:**

Having peered into the various principles outlined by British and European data protection law, this paper can thus proceed to critically examine the current state of data protection within the Kenyan jurisdiction vis-à-vis the data protection regime present in Europe. This chapter will achieve the latter in three ways; through an incisive look into the Constitution and the Articles therein that may enable data protection legislation, through analyzing the Court's rationale in the decision of *Benard Murage v. Fineserve Africa Limited and Four Others (Petition No. 503 of 2014)* one of the Kenyan judiciary's encounters with a data-centric technology, and through analyzing the various data protection principles present within the African Union's Convention on Personal Data Protection and Cybersecurity.

**1. Constitutional Provisions and the Data Protection Agenda:**

The protection of the fundamental rights of her citizens is one of the essential functions of the State, and this mandate is certainly implemented by the Constitution of Kenya. Insofar as data protection is concerned, the Constitution outlines the following Articles in order to protect its citizens:

**1. The protection of fundamental rights:**

- a) Article 46: Consumer rights: The Constitution under Article 46 seeks to protect her citizens as consumers of various products and services in the Kenyan market. The latter has an immense effect in the provision of software goods and the participation of companies in the Kenyan Digital Market. According to the tenets of Article 46, Kenyans have the right to; goods and services of reasonable quality; the information necessary for them to gain full benefit from goods and services; the protection of their health, safety, and economic interests; and to compensation for loss or injury arising from defects in



goods or services.<sup>220</sup> To these ends, Parliament is expected to enact legislation to provide for consumer protection and for fair, honest and decent advertising. Moreover, Article 46 applies to goods and services offered by public entities or private persons.

The fact that the Constitution points out that every citizen is entitled to the protection of their health, safety and economic interests as consumers, lucidly justifies the need for data protection regulation within the State. As cybercriminals ravage technology businesses and extract valuable data regarding various enterprises, the economic interests of these corporations and their clientele are singularly and jointly affected. Moreover, the guarantee accorded to consumers for compensation in the event of loss or injury from defective goods and services may ultimately justify consumer claims for losses sourcing from the effects of unprotected databases by vendors. An example would be the extraction of contact details from the numerous money transfer services offered in Kenya by service providers, leading to the eventual siphoning of monies from affected accounts. The account holders in the set up outlined are provided with a sovereign basis to claim for such costs. Similarly, the Constitution also broadly allows any injury caused by the consumption of goods and services to be worth compensation.<sup>221</sup> This also poses a problem for software enterprises, as claims regarding libel and injury of reputation due to the breach of their security databases and/or use of their software products could be substantiated by this provision. Further, the implementation of these consumer rights are not limited to private enterprises and rightly so. Public entities are also expected to safeguard consumers from loss or injury from use of their products, digital or otherwise<sup>222</sup>.

Parliament, according to Article 46, has also been placed with the significant responsibility of developing the appropriate consumer protection framework for the benefit of her citizens. It is disappointing to note that the protection of the data integrity of consumers within the Republic of Kenya has not been in any way legislated against in the Consumer Protection Act. It is vital that the data derived from consumers be

---

<sup>220</sup> Article 46, Constitution of Kenya (2010)

<sup>221</sup> Article 46, The Constitution of Kenya (2010)

<sup>222</sup> Article 46, The Constitution of Kenya (2010)



protected, as it may be just as valuable to market producers (if not more) and its protection could go a long way in fulfilling the government's dual mandate of protecting citizens' fundamental rights while facilitating economic growth.

- b) Article 31: Privacy: Under Article 31, every person has the right to privacy, which includes the right not to have information relating to their family or private affairs unnecessarily required or revealed; or the privacy of their communications infringed.<sup>223</sup> The latter has been established as a universal and fundamental right, and can thus be seen in Article 8 of the Charter of the Fundamental Rights of the European Union. This has impacted data protection regulation as individual rights are heavily considered in European legislation. Similarly, the right to privacy within the Kenyan jurisdiction necessitates the implementation of sound data protection policies to protect the family life and correspondence of each individual within the State.

## 2. Jurisdiction:

- a) Article 22: Under Article 22(1), every person has a right to institute court proceedings claiming that a right or fundamental freedom in the Bill of Rights has been denied, violated or infringed, or is threatened.<sup>224</sup> This enables users of digital products and services to seek legal redress for any violation of their fundamental rights through the Kenyan justice system. Further, under Article 22(4), the absence of rules establishing a fair, neutral and knowledgeable adjudication process does not hinder the administration of justice through the judicial process. In essence, the lack of the appropriate data protection regulatory framework in no way hinders the assertion and protection of one's fundamental rights in a Kenyan Court of Law.

It is interesting to note that in the case of *Coalition for Reforms and Democracy v Attorney General*<sup>225</sup>, the Court interpreted the use of the term, 'threatened' in Article 22 to expressly state that for relief to be granted by the Court, it is not necessary for the

---

<sup>223</sup> Article 31, Constitution of Kenya (2010)

<sup>224</sup> Article 22(1), Constitution of Kenya (2010)

<sup>225</sup> *Coalition for Reforms and Democracy v Attorney General*(Petition No.630 of 2014)



actual breach of the Constitution or violation of fundamental freedoms to be evidenced, but rather that such violation or breach could be imminent.

- b) Article 165: Article 165(3) establishes the High Court's jurisdiction to determine matters where a right or a fundamental freedom in the Bill of Rights has been denied, violated or infringed. With this Statute, it can be evidenced that in the absence of a determined data protection tribunal, the Kenyan Constitution has enabled the High Court to adjudicate over such violations. This determination will be made clear by the analysis of *Benard Murage v. Fineserve Africa Limited and Four Others* further in this chapter.
- c) Article 258: Under Article 258(1), The Constitution states that every person has the right to institute court proceedings, claiming that it has been contravened, or is threatened with contravention. Moreover, under (2), In addition to a person acting in their own interest, court proceedings under clause (1) may be instituted by a person acting on behalf of another person who cannot act in their own name; a person acting as a member of, or in the interest of, a group or class of persons; a person acting in the public interest; or an association acting in the interest of one or more of its members.

## **2. Petition No. 503 of 2014: An analysis of the interaction of the Kenyan legal regime and emergent, data-centric technologies:**

### **A. Introduction:**

The iconic case of *Benard Murage versus Fineserve Kenya Limited, Equity Bank Limited, The Communications Authority of Kenya and the Central Bank of Kenya* (The 1<sup>st</sup>, 2<sup>nd</sup>, 3<sup>rd</sup> and 4<sup>th</sup> respondents respectively) plays the crucial role of showcasing Kenya's current state of data protection regulation. Moreover, it highlights the various measures undertaken by local legislation to protect the nation's data integrity and the interaction of these local measures with international standards.

The basis for the Petition lay on the introduction of a new technology by the 2nd Respondent known as Thin SIM (Subscriber Identity Module) Technology which entails overlaying a SIM card on a pre-existing SIM card belonging to a third party. The thin SIM sits between the microchip of the primary SIM card and the SIM card socket of a mobile handset and





allegedly has visibility of all communications taking place between the primary SIM and the mobile handset.

It was therefore the Petitioner's case that if the Respondents are not restrained from the roll out of the Thin SIM technology, the security of his personal data would not be guaranteed and in his Petition dated 10th October, 2014, he has sought the following orders;

- a) That the Honorable Court be pleased to issue a declaration that Article 31(c) and 31(d) is in force and is mandatory that for its realization a data protection law be enacted.
- b) A conservatory order be issued restraining the 1st Respondent and 2nd Respondent from rolling out the thin sim technology pending the enactment of a data protection law.
- c) A conservatory order be issued restraining the 3rd Respondent & 4th Respondent from issuing any decision or directive in respect to the thin sim technology rollout by the 1st and 2nd Respondents pending the final determination of this case.
- d) That the Honorable Court be pleased to award the Petitioners costs of and incidental to these proceedings.
- e) The Honourable Court be pleased to make any order as it seems just.”

A. The Petitioner's submissions:

- The petitioner deponed that he was an account holder with the 2nd Respondent and was a member of the public whose personal data is held by the 2nd Respondent. That the Thin SIM technology worked by making the Thin SIM sit between the microchip of the primary SIM card and the SIM card socket of a mobile phone handset and has visibility of all communications taking place between the Primary SIM and the mobile handset thus exposing it to man-in-the-middle attacks including personal data contamination and access by third Parties. He also pointed out that the Thin SIM is also capable of remote communication through its contactless communication capabilities, thus enhancing its general capabilities.<sup>226</sup>
- He also averred that the Global System for Mobile Communication Association (GSMA) is an association and not a regulatory body and therefore the 1st and 2nd

---

<sup>226</sup> Petition No. 503 of 2014, para 2.



Respondents needed to undertake further regulatory measures before the roll out of the Thin SIM and not merely rely on GSMA's approval of the same. He maintained that the Thin SIM had security vulnerabilities and the 3rd Respondent had placed a tender for consultancy services to undertake evaluation performance and security features on the Thin SIM in appreciation of that fact.<sup>227</sup>

- It was his further position that the Thin SIM technology has not been used in Countries with large scale money transfer services and in countries where the Thin SIM technology has been used, data protection laws have been enacted.<sup>228</sup>As regards the current money banking services, he stated that the 2nd Respondent has been using existing GSM services and not the Thin SIM technology to provide those services.<sup>229</sup>
- He also claimed that countries that have been said to use the Thin SIM primarily use it for voice and data roaming services and not large scale mobile money transfer services as is proposed in Kenya.<sup>230</sup>
- Further, that the roll out of the Thin SIM technology has been halted by the Parliamentary Committee on Energy and Information and Communication based on privacy and data protection and this Court ought to do the same
- Mr. Kirwa presented the Petitioner's case and submitted that the thin SIM technology as manifested from its functionality, provided a real threat to the Petitioner's enjoyment of his rights under Article 31 (c) and (d) of the Constitution in so far as his personal data is concerned. That his fears are founded on the security vulnerabilities of the Thin SIM which transcends the scope of the user by making it possible for personal and sensitive data such as PIN numbers.
- He also submitted that due diligence was not conducted before introducing the thin SIM and that had that been done, then the issue of the functionality of the thin SIM would have been detected from its patent and used encryption keys to be accessed by third parties, to his prejudice.

---

<sup>227</sup>Petition No. 503 of 2014, para. 2.

<sup>228</sup>Petition No. 503 of 2014, para. 2

<sup>229</sup>Petition No. 503 of 2014, para. 2

<sup>230</sup>Petition No. 503 of 2014, para.2



- On the competence of the Petition, he claimed that the issues raised in the Petition are real and not hypothetical as alleged by the Respondents. That the Court had the jurisdiction to defend the Constitution and to inquire into the threat of violation of right to privacy and under international law, Kenya has an obligation to adopt legislative and other measures to give effect to the prohibition against interferences and attacks to the protection of the right to privacy. That in recognition to that role, the Attorney General has published the Data Protection Bill 2012, whose objects are clear but has yet to become law.
- It was Mr. Kirwa's further submission that Parliament had halted the roll out of the thin SIM technology pending satisfaction as to its security and functionality. That the 3rd Respondent cannot defy Parliament as the latter exercises oversight over it, and further submitted that Parliament was justified in halting the roll out as guardians of public interest.
- Counsel for the petition also submitted that the violations of the Petitioner's right to privacy and consumer protection are constitutional issues which this Court is enjoined to safeguard and protect and that recourse for violation of constitutional rights lies to the High Court and not a tribunal as alleged by the Respondents. He thus submitted that the doctrine of constitutional avoidance did not apply in this Petition and that the Court should exercise its powers and strike a balance to ensure that the constitutional safeguards in Article 31(c) and 31 (d) of the Constitution are upheld.

**B. The Court's Determination:**

With relevance to the dissertation topic, the following three paint points of data protection regulation were addressed by the Court in this matter. First, the Court pointed out the various dispute resolution mechanisms made available by statute in the event of such a petition. Secondly, the Court determined the petitioner's right to institute proceedings against the respondents, and finally, the Court asserted whether the petitioner's right to privacy was indeed violated, or under impending threat of violation.<sup>231</sup>

---

<sup>231</sup> Petition No. 503 of 2014, para. 2



- i) Whether there are alternative dispute resolution mechanisms in the event of such a petition:

The Respondents submitted that this Court has no jurisdiction to determine the Petition because the dispute herein is one which ought to be determined by the Appeals Tribunal created under the Kenya Information and Communication (Amendment) Act, 2013 and also the dispute resolution mechanism established under the Consumer Protection Act, 2012. The Court asserted that there existed an Appeals Tribunal, established under Section 102(1) of the Kenya Communications Act which provides as follows;

*“There shall be established an Appeals Tribunal for the purpose of arbitrating in cases where disputes arise between the parties under this Act and such matters as may be referred to it by the Minister”.*

The Court further stated that there exists a chain of authorities from the High Court as well as the Court of Appeal that: where a statute has provided a remedy to a party, this Court must exercise restraint and first give an opportunity to the relevant bodies or State organs to deal with the dispute as provided in the relevant statute. This principle was well articulated by the Court of Appeal in *Speaker of National Assembly v Njenga Karume [2008]*<sup>232</sup>, where it held that;

*“In our view there is considerable merit.....that where there is clear procedure for the redress of any particular grievance prescribed by the Constitution or an Act of Parliament, that procedure should be strictly followed.”*<sup>233</sup>

The same principle has been underlined in the cases of *Kipkalya Kones v Republic & Another ex parte Kimani Wanyoike & 4 Others (2008) 3 KLR (EP) 291*, *Francis Gitau Parsimei & 2 Others v National Alliance Party & 4 Others Petition No.356 and 359 of 2012*.

Further, the Court stated that it was bound to follow that principle of law since it flows from the other important principle that not each and every violation of the law must be raised before the High Court as a constitutional issue. Where there exists an alternative remedy

<sup>232</sup>Speaker of National Assembly v Njenga Karume [2008] 1 KLR 425,

<sup>233</sup>Speaker of National Assembly v Njenga Karume [2008] 1 KLR 425,



through statutory law, then it is desirable that such a statutory remedy should be pursued first.<sup>234</sup>

The Court also considered the jurisprudence from the case of *Damian Belfonte v The Attorney General of Trinidad and Tobago (2004)*<sup>235</sup>, which stated that where there is a means of redress that is inadequate, the Court should not exercise restraint. The Court stated that;

*“The opinion in Jaroo has recently been considered and clarified by the Board in A.G vs Ramanoop. Their lordships laid stress on the need to examine the purpose for which the application is made in order to determine whether it is an abuse of process where there is an available common law remedy. In their lordship’s words: “Where there is a parallel remedy, constitutional relief should not be sought unless the circumstances of which the complaint is made include some feature which makes it inappropriate to take that course. As a general rule, there must be some feature, which, at least arguably, indicates that the means of legal redress otherwise available would not be adequate. To seek constitutional relief in the absence of such a feature would be amiss, or abuse, of the Court’s process. Atypical, but by no means exclusive, example of such a feature would be a case where there has been an arbitrary use of state power. Another example of a special feature would be a case where several rights are infringed, some of which are common law rights and some for which protection is available only under the constitution. It would not be fair, convenient or conducive to the proper administration of justice to require an applicant to abandon his constitutional remedy or to file separate actions for the vindication of his rights”.*”

Drawing from these sentiments, The Court asserted its mandate to examine whether the alternative remedy provides an efficacious and satisfactory answer to the litigant’s grievance. In that regard, the Petitioner had filed this Petition pursuant to the provisions of Articles 22, 23 and 165(3) (b) of the Constitution which grants every person the right to institute Court

---

<sup>234</sup> See *Harrkinson v Attorney General of Trinidad and Tobago* [1980] AC 265, where the court concluded thus, “The mere allegation that a human right has been or is likely to be contravened is not itself sufficient to entitle the applicant to invoke the jurisdiction of the court under the section if it is apparent that the allegation is frivolous, vexatious or abuse of the process of court, as being made solely for the purpose of avoiding the necessity of applying the normal way for appropriate judicial remedy for unlawful administrative action which involves no contravention of any human right or fundamental freedom.”

<sup>235</sup> *Damian Belfonte v The Attorney General of Trinidad and Tobago* C.A 84 of 2004,



proceedings claiming that a right or fundamental freedom has been violated or is threatened with an infringement. That right, to access this Court, could thus not be impeded or stifled in a manner that frustrates the enforcement of fundamental rights and freedoms except in the circumstances noted in *Belfonte*.<sup>236</sup>

Hence, the Court pointed out that the question brought before the Court was not whether the rollout of thin-SIM technology is proper or not but whether that action would violate the Petitioner's rights under Articles 31 and 46 of the Constitution, (right to private and consumer rights, respectively). The mandate and jurisdiction to determine that question lies in this Court under Articles 22, 23(3) and 165(3) (d) of the Constitution. This effectively meant that the Appeals Tribunal established under the Kenya Information and Communication Act does not have the jurisdiction to determine alleged violations of the Constitution. This position was also asserted by the Court in the case of *Wananchi Group (Kenya) Ltd v The Communications Commission of Kenya*.<sup>237</sup>

In conclusion, the Court referred to the judgement of Majanja J J in *Isaac Ngugi v Nairobi Hospital and Another*<sup>238</sup> stated as follows;

*“For instance, the Court will be reluctant to apply the Constitution directly to horizontal relationships where specific legislation exists to regulate the private relations in questions. In other cases, the mechanisms provided for enforcement are simply inadequate to effectuate the Constitutional guarantee even though there exists private law regulating a matter within the scope of the Application of the Constitutional right or fundamental freedoms. In suchcases, the Court may proceed to apply the provisions of the Constitution directly.”*

ii) Whether the petitioner is a proper party to these proceedings:

It was the 2<sup>nd</sup> Respondent's submission that the Petitioner did not have any interest in the rolling out of the Thin SIM technology capable of protection by the Court, as he was not an account holder with the 2<sup>nd</sup> Respondent and as such he could not to be affected by the said

<sup>236</sup> Petition No. 503 of 2014, para. 3

<sup>237</sup> *Wananchi Group (Kenya) Ltd v The Communications Commission of Kenya* Petition No.98 of 2012

<sup>238</sup> *Isaac Ngugi v Nairobi Hospital and Another* (Petition No.461 of 2012)



Thin SIM technology. The Court however rebutted this assumption by asserting that the Petitioner did not need to act on his behalf in order to institute court proceedings to establish that tenets of the Constitution have been contravened or are in threat of contravention. The latter is expressly stated by Article 258(2).

As such the Court held that the Petitioner was accorded the right to institute such proceedings by the Constitution itself, in this regard, Lenaola J. expressly stated:

*“In the totality of evidence before me, while I am inclined to find that the Petitioner is not an account holder with the 2nd Respondent, under Article 258 (2) he can institute Court proceedings claiming a violation of the Constitution generally and even in the public interest. He alleged in that regard that the present Petition has been filed on behalf of all account holders with the 2nd Respondent and whose information/data is subject to compromise and contamination through the use of the Thin SIM technology. If that is the case, I do not see any valid reason as to why I should find that the Petitioner is not the right party in these proceedings.*

iii) Whether the right of privacy is in threat of violation:

The Court noted that the Petitioner did not challenge the issuance of the license to the 1<sup>st</sup> and 2<sup>nd</sup> Respondent and did not even challenge powers of the 3<sup>rd</sup> and 4<sup>th</sup> Respondents over the Thin SIM technology. The Court further noted that it did not hear the Petitioner accuse the 4<sup>th</sup> Respondent of any wrong doing. His case would therefore be seen through the prism of the alleged threat of right to privacy as provided for under Article 31 of the Constitution.

In that regard, he claimed that the rolling out of the Thin SIM technology would violate his right to privacy as it is suspect to interception and contamination of the primary SIM data. That was the issue that ran throughout his submissions and all other issues raised rotated around that singular complaint.

The Court noted that the right to privacy is provided for under Article 31 of the Constitution in the following manner;

*Every person has the right to privacy, which includes the right not to have –*



- a. *Their person, house or property searched;*
- b. *Their possessions seized;*
- c. *Information relating to their family or private affairs unnecessarily required or revealed;*  
*or*
- d. *The privacy of their communications infringed.*

In making its determination, the Court sought insight from the Irish Supreme Court in *Kennedy vs Ireland (1987)*<sup>239</sup>, who in addressing the said right, held that phone-tapping violated the right to privacy. Hamilton J made it clear in that case that the right to privacy must ensure the preservation of the dignity and freedom of the individual in a sovereign, independent and democratic society. In his view;

*“The dignity and freedom of an individual in a democratic society cannot be ensured if his communication of a private nature, be they written or telephonic, are deliberately, consciously and unjustifiably intruded upon and interfered with.”*

The Court also drew insight from the decision in *CORD v Attorney General (supra)* which held that surveillance and intercepting of communication violated the right to privacy. The Court expressed itself as follows;

*“We are clear in our minds that surveillance in terms of intercepting communication impacts upon the privacy of a person by leaving the individual open to the threat of constant exposure. This infringes on the privacy of the person by allowing others to intrude on his or her personal space and exposing his private zone.”*

With these principles in mind, the Court then turned to determine whether the right of privacy was in any impending threat of violation. The starting point was seen to be the Affidavit of Perminus Karungu where he explained that the Thin SIM technology entailed the issuance of a paper Thin SIM card that was embedded with a chip whereby users thereof would overlay it on their primary SIM card, regardless of network and has the capability of a

---

<sup>239</sup>*Kennedy vs Ireland (1987) I.R 587*





dual SIM phone without having an actual dual SIM phone. The 1st and 2nd Respondents also averred in the Affidavit of John Waweru that the Thin SIM only relies on the primary SIM for anchorage and space in the mobile handset and does not technically have the capacity to interfere or intercept the services or connections of the Primary SIM. Further, that it was incapable of remotely connecting to outside sources for additional resource without the knowledge of the user.

In determining the true and factual position regarding the technical aspects of the case, the Court would resort to the answers given by the 3<sup>rd</sup> Respondent since it is the body established under the Kenya Information and Communication Act, to undertake licensing and regulation of telecommunication as well as radio communications and postal services in Kenya. In addressing that issue, the 3<sup>rd</sup> Respondent engaged licensed Mobile Network Operators and Mobile Virtual Network Operators in a discussion with a view to making a decision on the matter; It also enjoined the 4<sup>th</sup> Respondent in the discussion due to the complaint touching on mobile money transfer services. In addressing the said issue it also scrutinized the Taiwanese Company, Taisys Technologies Company Ltd which manufactures the Thin SIM. It went further and obtained the opinion of the GSMA, an association of mobile operators and related companies devoted to supporting the standardizing, deployment and promotion of the GSM mobile telephone system, which recommended that before the Thin SIM card could be used in the market, the 3<sup>rd</sup> Respondent should ensure the following;

*“(a) Promoters and issuers of the thin SIM card should provide assurances on verification of the modes applied to mitigate the risks.*

*(b) That the overlay SIM technology should have been independently analyzed and certified as being free from any functionality capable of undermining the security of users and issuers of the small original SIMs; and*

*(c) Mobile phone users should be advised of the potential dangers that could result from inserting unapproved elements in their devices and they should be provided with assurances pertaining to approved solutions.”*



Following the above opinion, the 3<sup>rd</sup> Respondent benchmarked the Thin SIM against various standards, organizations and regulatory experts and carried out research to find out the global practices concerning the overlay SIM technology. Counsel for the 3<sup>rd</sup> Respondent explained that it established the following;

*“(a) [The] SIM overlay technology was developed nearly 10 years ago in China as a multi-operator access solution and it was primarily designed to avoid roaming fees;*

*(b) As a roaming tool, the Thin SIM card will elect to become the primary SIM card while roaming thus interfacing with local carriers at rates far better than the primary carrier;*

*c. The Canadian company, Roamly and American Company, Know Roaming, use the same technology presently to offer a low cost roaming service for their customers;*

*d. In China particularly the technology is additionally being used for financial services;*

*e. Research showed that the SIM overlay technology used in mobile banking was safe since it used the SMS channel as opposed to the modern mobile applications over internet; and*

*f. Further, it emerged that the technology is operational in both smart and functional phones thus easily available to low income clients.”*

Following the above report, the 4<sup>th</sup> Respondent held a stakeholder conference at the Authority’s offices and the participants included the four Mobile Network Operators in Kenya i.e Safaricom, Airtel Kenya, Yu Mobile and Orange Telkom, the 1<sup>st</sup> Respondent, the 2nd Respondent and Taisys Technologies among others. It was observed in that stakeholder conference that;

*“(i) The Thin SIM complies with all minimum mandatory international standards pertaining to the manufacturing of the Thin SIM;*

*ii. No major complaints particularly none on interception of traffic of the primary SIM card has been reported so far;*



*iii. Tests conducted on Taisys Thin SIM by China National Computer Quality Supervising Test Center as well as the Bank Card Test Centre of China show that the Thin SIM complies with applicable ISO and European Telecommunications Standards Institute standards; and*

*iv. Based on the opinion of GSMA, save for the inherent vulnerabilities of all SIM cards, there are no specific and confirmed vulnerabilities arising from the use of the ThinSIM.”*

On the basis of the above findings, the 3rd Respondent decided as follows;

*“(a) There were no sufficient grounds that can hinder the entry of the Thin SIM into the Kenyan market.*

*b. The Authority will allow the use of the Thin SIM technology under strict observation for a period of one year. During his period, only Taisy’s Thin SIM will operate in the Kenyan market;*

*(c) The Authority will hire an internationally reputable firm to conduct a security audit on all SIM cards and in particular the use of the Thin SIM in mobile money transfer services, and recommend a framework for regulating the use of SIM card in Kenya during this period;*

*(d) During the one year testing period, if any vulnerability is discovered from the use of Taisy’s Thin SIM card, then operations of the Thin SIM card in the Kenyan market will cease immediately pending the final recommendations from the security report; and*

*(e) Operators intending to use the Thin SIM for mobile money transfers must obtain authorization from Central Bank of Kenya.”*

Perminus Karungu, Counsel for the 3<sup>rd</sup> Respondent therefore deponed that the 3rd Respondent’s authority to grant a limited approval for the use of the Thin SIM card was also in tandem with the advice of GSMA in the following manner;

- Allowing the use of the Thin SIM cards manufactured by Taisy’s Technologies as the same had been independently verified and found to comply with the standards required for use in the banking industry.



- Its use would be under strict observation of internationally reputable financial security firm; and
- All the entities that would use the Thin SIM card were required to provide assurances that they have put in place the requisite security measures and to that end, it has made it mandatory for the said entities to provide an undertaking indemnifying not only the authority for any liabilities that may be confirmed but also, the entities are required to meet any liabilities suffered by consumers who experience manipulation or blocking of communications of the Primary card.

The Court asserted that the 3<sup>rd</sup> Respondent, as a regulator, had already resolved a complaint similar to the one before it regarding the use of Thin SIM technology. The Court also emphasized that the 3<sup>rd</sup> Respondent as the regulator of Mobile Network Operators and Mobile Network Virtual Operators and the 4<sup>th</sup> Respondent as the regulator of mobile banking in Kenya are the best judges to determine the merits pertaining to the complaint made now by the Petitioner and not the Court. Parliament has set out the law and the power of formulating policy in respect to regulating communication and has conferred such power to the 3<sup>rd</sup> Respondent and mobile banking to the 4<sup>th</sup> Respondent and it would be wrong, according to the Court for it to intervene as to the merits of the decision already made by the 3<sup>rd</sup> and 4<sup>th</sup> Respondents as the Regulators. The Court stated that it could only intervene in very limited circumstances and in the clearest of cases for instance where it is being alleged that there is abuse of discretion, or that the decision makers have exercised their discretion for an improper purpose or have acted unfairly or in excess of their statutory mandate, which was not the case in the petition brought before it. Its verdict was in accordance with the *Republic v The Council of Legal Education ex parte James Njuguna and 14 Others*.<sup>240</sup>

Therefore, The Court pointed out that it was not demonstrated that the 3<sup>rd</sup> Respondent exercised its powers arbitrarily. On the contrary, The Court was satisfied that the decision it reached was made pursuant to its mandate which is within the letter, the purpose and objects of the Kenya Information and Communication Act including the applicable Regulations. That being so, the

---

<sup>240</sup>*Republic v The Council of Legal Education ex parte James Njuguna and 14 Others*, Misc. Civil Case No. 137 of 2004 (unreported).



Court had no reason to intervene in a manner that interfered with the merit of a decision clearly falling within the relevant statutory agency without allegations of any irregularities on its part. It therefore followed that from the findings of all the technical bodies named in the Petition, the Thin SIM technology was deemed safe in banking as proposed and any risks would be dealt with by the relevant bodies. Moreover, measures were undertaken by the 3<sup>rd</sup> Respondent wherein the Thin SIM technology would undergo strict surveillance by an internationally reputable financial security firm for a period of one year. During the latter period, there existed an indemnification process in the event of loss or injury due to the use of the Thin SIM technology by consumers.

As such, the Court found that the alleged threat to the right of privacy has not been proven and the Petitioner's complaints in that regard were summarily dismissed.

In his ratio, Justice Lenaola J stated:

*"Lastly, I do not see any reason and I have said why above that I should halt the roll out of the Thin SIM technology pending the enactment of the Data Protection Bill into law. This Court can only interfere with the legislative process of Parliament especially before Parliament has concluded its deliberations on a Bill in very rare cases. The issue whether a data protection law is necessary as a safeguard to the use of the Thin SIM is not one such case. This Court cannot order Parliament to make specific laws but only test both the process leading to those laws and their contents against the constitutional muster. What has been placed before this Court is a Bill and in that case it is not clear what the end result of that Bill would be and I will therefore exercise judicial restraint and avoid making any orders in that regard."*<sup>241</sup>

The conclusion of the Court's judgement notably asserted the lack of data protection regulation within current Kenyan legislation, however, a Data Protection Bill is in the pipeline and may play the crucial role of entrenching data protection regulation and practice within our jurisdiction. It is fundamental to note that the constitutionality of any regulations so passed by Parliament can be reviewed by the able arm of the Judiciary and as such any data protection regulation that may harm or threaten the fundamental rights of any Kenyan citizen can be

---

<sup>241</sup> Petition No. 504 of 2014, judgement of Justice I. Lenaola.



withdrawn from adjudication in the Kenyan courts. As such, the Judiciary remains a sentinel to the data integrity of her citizens.

**3. The African Union Convention on Personal Data Regulation and Cybercrime:  
Insights into the imminent African Data Protection Regime:**

**1. Introduction:**

The adoption of digital technologies within the African continent and the proliferation of data-centric businesses in Africa has not gone unnoticed by Member States of the African Union. According to the Preamble of the African Union Convention on Personal Data Regulation and Cybercrime, the Convention was drafted in fulfilment of the intention to create the African Union's Information Society, a body which is intended to strengthen existing legislations on Information and Communication Technologies of Member States and their respective economic communities. Further, the Convention was drafted in order to establish the appropriate regulatory framework on cyber-security and personal data protection takes into account the requirements of respect for the rights of citizens, guaranteed under the fundamental texts of domestic law and protected by international human rights Conventions and Treaties, particularly the African Charter on Human and Peoples' Rights.<sup>242</sup>

The Member States of the African Union also enacted data protection regulations in order to facilitate the development of the knowledge economy within Africa. In its Preamble, the Convention highlights the major obstacles to the development of electronic commerce in Africa are linked to security issues, particularly the gaps affecting the regulation of legal recognition of data communications and electronic signature; the absence of specific legal rules that protect consumers, intellectual property rights, personal data and information systems; the absence of e-services and telecommuting legislations; the application of electronic techniques to commercial

---

<sup>242</sup> Preamble of the African Union Convention on Personal Data Regulation and Cybercrime.



and administrative acts; the probative elements introduced by digital techniques (time stamping, certification, etc.); the rules applicable to cryptology devices and services; the oversight of on-line advertising and the absence of appropriate fiscal and customs legislations for electronic commerce.<sup>243</sup>

Fundamentally, the Member States of the Union drafted the Convention due to the urgent need to establish a mechanism to address the dangers and risks deriving from the use of electronic data and individual records, with a view to respecting privacy and freedoms while enhancing the promotion and development of ICTs in the Member States of the African Union. It can thus be concluded that the goal of the Convention is to address the need for harmonized legislation in the area of cyber security in Member States of the African Union, and to establish in each State party a mechanism capable of combating violations of privacy that may be generated by personal data collection, processing, transmission, storage and use. The Convention meets this end by proposing a type of institutional basis, wherein the Convention guarantees that whatever form of processing is used shall respect the basic freedoms and rights of individuals while also taking into account the prerogatives of States, the rights of local communities and the interests of businesses.<sup>244</sup> Finally the Convention seeks to necessitate the adoption of internationally recognized best practices in order to guarantee the data integrity of the Member States' citizens<sup>245</sup>.

## **2. The principles of data protection regulation present in the AU Convention on Personal Data Protection and Cybercrime:**

### **I. The establishment of National Personal Data Protection Authorities:**

Under Article 11 of the Convention, Each State Party shall establish an authority in charge of protecting personal data. The national protection authority should be an independent administrative authority with the task of ensuring that the processing of personal data is conducted in accordance with the provisions of the Convention. The national protection authority is expected to inform its citizens and the processing officials of their rights and obligations.

---

<sup>243</sup>Preamble of the African Union Convention on Personal Data Regulation and Cybercrime

<sup>244</sup>Preamble of the African Union Convention on Personal Data Regulation and Cybercrime

<sup>245</sup>Preamble of the African Union Convention on Personal Data Regulation and Cybercrime



Further, each State Party is free to determine the composition of the national personal data protection authority. Note that the latter occurs without prejudice to Article 11.6, which points out that membership of the national protection authority should be incompatible with membership of Government, carrying out the functions of business executive and ownership of shares in businesses within the information and communication technologies sector.<sup>246</sup>

Without prejudice to national legislations, members of the national data protection authority are expected to enjoy full immunity for opinions expressed in the pursuit, or in connection with the pursuit of their duties. Members of the national protection authority shall not receive instructions from any other authority in the performance of their duties. The latter tenets are meant to guarantee the independence of the data protection authority from the undue pressures of the State government, in order to guarantee the safety of the fundamental rights of Member States' citizens. Note that this clause can be limited by the legislation present in local jurisdictions.

Article 12 of the Convention outlines the various duties and powers of national data protection authorities within Member States' local jurisdiction. According to Article 12, the national protection authorities are expected to ensure that the processing of personal data is consistent with the provisions of this Convention within State Parties of the African Union. The national protection authorities have the mandate to ensure that Information and Communication Technologies do not constitute a threat to public freedoms and the private life of citizens. To this end, they are responsible for:

- Responding to every request for an opinion regarding personal data processing;
- Informing the persons concerned and data controllers of their rights and obligations;
- In a number of cases, authorize the processing of data files, particularly sensitive files;
- Receiving the preliminary formalities for personal data processing;
- Entertaining claims, petitions and complaints regarding the processing of personal data and informing the authors of the results thereof;

---

<sup>246</sup> Article 11 of the African Union Convention on Personal Data Regulation and Cybercrime.





- Speedily informing the judicial authority of certain types of offences that have come to their attention;
- Undertaking the audit of all processed personal data, through its officials or sworn officials;
- Imposing administrative and monetary sanctions on data controllers;
- Updating a processed personal data directory that is accessible to the public;
- Advising persons and bodies engaged in personal data processing or in carrying out tests and experiments likely to result in data processing;
- Authorizing trans-border transfer of personal data;
- Making suggestions that could simplify and improve legislative and regulatory frameworks for data processing;
- Establishing mechanisms for cooperation with the personal data protection authorities of third countries;
- Participating in international negotiations on personal data protection;
- Preparing an activity report in accordance with a well-defined periodicity, for submission to the appropriate authorities of the State Party.<sup>247</sup>

Further, in the event of breach of data protection standards and regulations, the national protection authorities may decide on the following measures; the issuance of warning to any data controller that fails to comply with the obligations resulting from this Convention or the issuance of an official warning letter to stop such breaches within a timeframe set by the authority. Where the data controller fails to comply with the official warning letter addressed to him/her, the national protection authority may impose the following sanctions after adversarial proceedings: temporary withdrawal of the authorization granted; permanent withdrawal of the authorization or a monetary fine.

In cases of emergency, where the processing or use of personal data results in violation of fundamental rights and freedoms, the national protection authority may, after adversarial proceedings, decide as follows: Discontinuation of data processing; Blocking of some of the

---

<sup>247</sup> Article 12 of the African Union Convention on Personal Data Regulation and Cybercrime.



personal data processed; Temporary or permanent prohibition of any processing at variance with the provisions of this Convention. Note that, as per Article 12, the sanctions imposed and decisions taken by national protection authorities are subject to appeal.

II. The principle of consent and legitimacy of data processing:<sup>248</sup>

According to Article 13, the processing of personal data shall be deemed to be legitimate where the data subject has given his/her consent. This requirement of consent may however be waived where the processing is necessary for:

- a) Compliance with a legal obligation to which the controller is subject;
- b) Performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed;
- c) Performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- d) Protect the vital interests or fundamental rights and freedoms of the data subject.

III. The principle of lawfulness and fairness of personal data processing:<sup>249</sup>

According to Article 13 of the Convention, The collection, recording, processing, storage and transmission of personal data should be undertaken lawfully, fairly and non-fraudulently.

IV. The principle of purpose, relevance and storage of processed personal data<sup>250</sup>:

In accordance with Article 13 of the Convention, Data collection shall be undertaken for specific, explicit and legitimate purposes, and not further processed in a way incompatible with those purposes. Data collection should be adequate, relevant and not excessive in relation to the purposes for which they are collected and further processed. Data should be kept for no longer than is necessary for the purposes for which the data were collected or further processed. Beyond the required period, data may be stored only for the specific needs of data processing

---

<sup>248</sup> Article 13 of the African Union Convention on Personal Data Regulation and Cybercrime.

<sup>249</sup> Article 13 of the African Union Convention on Personal Data Regulation and Cybercrime.

<sup>250</sup> Article 13 of the African Union Convention on Personal Data Regulation and Cybercrime.



undertaken for historical, statistical or research purposes under the law.

V. Principle of accuracy of personal data:<sup>251</sup>

Data collected should be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified.

VI. Principle of transparency of personal data processing:<sup>252</sup>

The principle of transparency requires mandatory disclosure of information on personal data by the data controller.

VII. Principle of confidentiality and security of personal data processing:<sup>253</sup>

- a) Personal data shall be processed confidentially and protected, in particular where the processing involves transmission of the data over a network;
- b) Where processing is undertaken on behalf of a controller, the latter shall choose a processor providing sufficient guarantees. It is incumbent on the controller and processor to ensure compliance with the security measures defined in this Convention.

VIII. The processing of sensitive data<sup>254</sup>:

In accordance with Article 14 of the Convention, State Parties are expected to actively prohibit any data collection and processing revealing racial, ethnic and regional origin, parental filiation, political opinions, religious or philosophical beliefs, trade union membership, sex life and genetic information or, more generally, data on the state of health of the data subject.

However, the latter statute cannot be applied to categories where:

---

<sup>251</sup> Article 13 of the African Union Convention on Personal Data Regulation and Cybercrime

<sup>252</sup> Article 13 of the African Union Convention on Personal Data Regulation and Cybercrime

<sup>253</sup> Article 13 of the African Union Convention on Personal Data Regulation and Cybercrime

<sup>254</sup> Article 14 of the African Union Convention on Personal Data Regulation and Cybercrime



- Processing relates to data which are manifestly made public by the data subject;
- The data subject has given his/her written consent, by any means, to the processing and in conformity with extant texts.
- Processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his/her consent;
- Processing, particularly of genetic data, is required for the establishment, exercise or defense of legal claims;
- A judicial procedure or criminal investigation has been instituted;
- Processing is necessary in the public interest, especially for historical, statistical or scientific purposes;
- Processing is necessary for the performance of a contract to which the data subject is party to or in order to take steps at the request of the data subject prior to entering into a contract;
- Processing is necessary for compliance with a legal or regulatory obligation to which the controller is subject;
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority or assigned by a public authority vested in the controller or in a third party to whom data are disclosed;
- Processing is carried out in the course of the legitimate activities of a foundation, association or any other non-profit making body with a political, philosophical, religious, cooperative or trade union aim, and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects

The Convention, under Article 14, legislates that personal data processing for journalistic purposes or for the purpose of research or artistic or literary expression shall be acceptable where the processing is solely for literary and artistic expression or for professional exercise of journalistic or research activity, in accordance with the code of conduct of these professions.

Note that under Article 14. 4, the Convention continues to expressly state that its provisions shall



not preclude the application of national legislations with regard to the print media or the audio-visual sector, as well as the provisions of the criminal code which provide for the conditions for exercise of the right of reply, and which prevent, limit, compensate for and, where necessary, repress breaches of privacy and damage to personal reputation.

According to Article 14.5 of the Convention, A person should not be subject to a decision which produces legal effects concerning him/her or significantly affects him/her to a substantial degree, which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him/her.

Crucially, the data controller should not transfer personal data to a non-Member State of the African Union unless such a State ensures an adequate level of protection of the privacy, freedoms and fundamental rights of persons whose data are being or are likely to be processed. The previous prohibition is not applicable where, before any personal data is transferred to the third country, the data controller has requested authorization for such transfer from the national protection authority.

Conclusion:

An analysis of the Convention reveals principles that remain at the heart of data protection laws to this day. In some respects, given that consistency is a quality much respected in law, this is a benefit. If consideration is given, however, to developments in computer technology in the last decade, problems may be identified. The Convention, a reflection of the current data protection law sourced principally from the Recommendations of the Council of Europe to the European Commission, is substantially based on the notion of a single controller with a single computer holding data.<sup>255</sup> This bears little resemblance to today's networked environment. In particular, reactive controls may not be sufficient. Once inaccurate data has found its way onto the Internet, the damage can never be undone. The initial Council of Europe resolutions did not attempt to prescribe the means by which Member States should give effect to the principles contained therein. As more and more European countries enacted data protection legislation, so too did the problems resulting from the international trade of information (frequently referred to as

---

<sup>255</sup> Lloyd J. Ian, *Information Technology Law, Sixth Edition* p. 24



transborder data flows) become more acute. The latter may be Africa's lot in the event that legislation governing transborder data flow is not better legislated against by the emergent Data Protection regime.

An apparent loophole in the Convention often criticised by human rights advocates can be seen in Article 14, which outlines that personal data should only be processed where the data subjects give express, unequivocal, free, specific, and informed consent.<sup>256</sup> However, the Convention adds an ominous exception, which outlines that such data protection can be limited in the case where access is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed. Given African States' putrid history of corruption and civic oppression, the latter may effectively empower governments to access sensitive data regarding State citizens for political reasons, or in the case of the justice system within the State, the deletion of evidence from private and public databases whose data may bear evidence implicating government agents engaged in rent seeking behaviour.

---

<sup>256</sup> See <https://www.accessnow.org/african-union-adopts-framework-on-cyber-security-and-data-protection/> (Accessed on 1/1/2016),



**CHAPTER FIVE: CONCLUSIONS AND RECOMMENDATIONS:**

**A. Recommendations:**

Following the various observations made by this paper, regarding the data protection regime in Africa and its effect of cloud-based technologies, this section will seek to offer recommendations that will better prepare the African Union for the integration and regulation of data-centric cloud-based technologies into their economies.

The recommendations has been divided into two sections. The first section regards cross-border data transfers whereby European law may offer valuable insights regarding regulation and restriction methods that can be assimilated into the current African Union data protection regime.

The second section intends to highlight the shortcomings of the current EU data protection regime, whose principles are present in the AU Convention, in order to draw remedial information on the disabilities of the currently designed data protection regime.

**1. Data Transfers & Their Regulation:**

An often understated feature of data protection, particularly in past legislative regimes, is the dynamic field of data transfers and their impact on emergent technologies. The interaction of data transfers and data protection is altogether problematic, as the globalization of the digital market needs to the use, sharing and application of different types of data across different jurisdictions the probability of export of illegal data continues to grow. In Europe, the Data Protection Directive and the Article 29 Working Party (A29WP) work hand in hand to ensure comprehensive data transfer through the European Economic Area.<sup>257</sup> This section will seek to unravel the various restrictions outlined by the Directive in order to outline a proper course of action for the adoption of data protection regulation in Africa.

Under Article 25(1), subject to certain derogations under Article 26,<sup>258</sup> Member States are forbidden from allowing a data controller to export personal data due to a ‘third country’ outside the European Economic Area, unless the country is seen to provide an adequate level of

---

<sup>257</sup> Millard C. *Cloud Computing Law*, Oxford Publishing Press (2013), p. 254

<sup>258</sup> Millard C. *Cloud Computing Law*, Oxford Publishing Press (2013), p. 254



protection for personal data, meaning a standard in keeping the Data Protection Directive's main principles. The latter applies whether the data are kept within the same entity, such as a subsidiary, or transferred to a company in the same group or an unrelated third party within the given jurisdiction.<sup>259</sup> The European Commission rationalized this tenet, as being fundamental to the adoption of data protection standards outside the European Economic Area. It is worth noting that this is an additional requirement, as a data export or transfer essentially constitutes 'processing', for which a legal justification is required according to the principles of data protection elaborated under Chapter 3, such as the data subject consent to processing, even where export is permitted under a derogation under Article 26.<sup>260</sup> It is the opinion of the writer that such a clause be inserted into the AU Convention on Protection of Personal Data and Cybercrime, wherein Member States are necessitated to adopt necessary adequacy requirements, as defined by the Convention. Moreover, the ban on data export should be implemented upon subsidiaries acting in Member States. Companies in default of this requirement should face punitive and where applicable, criminal liability in instances where they can be held to be liable to data export offences.

Under Article 25(6) of the Data Protection Directive, the European Commission can declare that certain States outside the European Economic Area have reached the adequacy standards set out by the Directive, and can thus receive personal data freely.<sup>261</sup> Examples of such countries include; Andorra, Argentina, Jersey, Israel, Guernsey, Isle of Man, New Zealand, Switzerland and Uruguay<sup>262</sup>. It is interesting to note that France and Spain have given their national data protection authorities the powers to make their own adequacy findings. The adjudication of such powers is immensely rare, moreover, no State has issued adequacy findings for countries not already declared as such by the European Commission.<sup>263</sup> In applying these findings to the case of the AU Convention, the writer would recommend the use of these differentiated standards according to market needs, by designing a benchmark as offered by the fundamental principles

---

<sup>259</sup> Kuner Christopher, *Transborder Data Flows and Data Privacy Law*. (Oxford: Oxford University Press, 2013). P. 25

<sup>260</sup> Millard C., *Cloud Computing Law*, p. 254

<sup>261</sup> Millard C., *Cloud Computing Law*, p. 254

<sup>262</sup> European Commission, '*Commission decisions on adequacy of the protection of personal data in third countries.*', (2013)

<sup>263</sup> Millard C., *Cloud Computing Law*, p. 255





present in the Convention, while balancing the latter against local statutes that may outline differentiated market needs.

Notably, the adequacy standards set by the Directive are explicitly defined as outlined by Article 25. However, in the African Union Convention on Personal Data Protection and Cybercrime, adequacy standards have not been so determined and as such can be a thorn in the side of national data protection regulators.<sup>264</sup> The latter may lead to the fragmentation of data protection regulations and differentiated standards. The latter may lead to slowed e-commerce activity and high transactional costs, hindering economic growth. Moreover, in the event of breach of data export restrictions, miscreants may escape justice due to the lack of set standards.

It is crucial to note that numerous cloud arrangements use remote data storage and other data processing, such that the geographic location of data and /or operations may 'change' as may 'change' as data may be replicated to equipment located in other countries, including third countries.<sup>265</sup> Therefore, the data export restriction within the current global data protection regime, poses significant problems to cloud providers, whose transactions by their nature involves data transfers from user to cloud {and vice versa), and automated data transfers within the cloud<sup>266</sup>. This technical reality could result in legal problems for data controllers established outside the EEA. This is because the Directive applies through Article (4)(1) not only to processing in the context of an EU establishment but also where a data controller based outside the EU is using 'equipment' or 'means' such as a cookie on the user's computer, or is using an EEA data centre or EEA provider<sup>267</sup>. These provisions thus develop a critical situation whereby a cloud provider with no establishment in the EEA may be subject to the EU data export regime when attempting to transfer data back from the EEA to its place of establishment or some other location outside the EEA, even if the data were originally collected outside the EEA and relates to non-EEA individuals. The inevitable result is that the Directive may ultimately lock out non-EEA cloud providers offering their services remotely to users in the EEA, unless they comply

---

<sup>264</sup>European Commission, 'Commission decisions on adequacy of the protection of personal data in third countries.'

<sup>265</sup>Cloud Computing Law, Christopher Millard, Oxford Publishing Press (2013), p. 255

<sup>266</sup>Cloud Computing Law, Christopher Millard, Oxford Publishing Press (2013), p. 255

<sup>267</sup> Cloud Computing Law, Christopher Millard, Oxford Publishing Press (2013), p. 230



with their adequacy requirements. Moreover, the enforceability of these EU Data Protection laws in practice seem questionable. The implication of these statutes in the sale of non-EEA technologies within the EEA seems adversely affected, as providers face stringent measures from local and regional data protection regulators prior to accessing the European Digital Market. In this regard, the writer opines that the development of model clauses within non-EEA provider enterprises will serve a fundamental function in allowing for their participation in the European Digital Market. Article 26 (4) provides that if a transfer of data to outside the EEA is made under the contractual clauses the terms of which have been approved by the European Commission for this purpose, the protection is considered adequate and the transfer must be permitted by Member States.<sup>268</sup> The European Commission have issued standard contractual clauses that fall within the latter statute, and their incorporation into cloud contracts may enable access into the lucrative European Digital Market. In a similar vein, this action could also apply to the function of the African Union in providing an efficient economic function to Member States, whereby standard contractual clauses can be designed for the purpose of cross border data transfers and the facilitation of data-centric businesses in our emerging economy. This will go a long way in maximizing returns for multinational companies and steering the economy in a positive manner.

The development of minimum standards in terms of anonymization and encryption in order to enable data export from various jurisdictions within the African Union can be seen to be fundamental to the development of cloud regulation and data protection within the Continent. Data fragments stored in the cloud may not be 'personal data' in the provider's hands if the provider is unable to read the fragments, although they would remain 'personal data' as regards the cloud user storing the data, who by logging into their account with the provider may reunite the non-identifiable fragments thus enabling them accessing into their data's specific identity-holder and function<sup>269</sup>. It seems then that in the event of strong encryption and/or anonymisation rendering the data unidentifiable, the issue of data protection does not arise as the data cannot be determined as personal. The implication of this policy will ultimately lead to sound data security infrastructure by application developers and cloud providers as well as Privacy by Design, as a norm and standard for enterprises in the technology space throughout the Continent.

---

<sup>268</sup> Data Protection Directive, Article 26(4)

<sup>269</sup> Millard C, *Cloud Computing Law*, p. 230



## **2. Lessons from the current data protection reform in the European Union:**

In 2014, the European Commission identified numerous shortcomings present in the then data protection regime, the very yardstick upon which the African Union's Convention on Personal Data Protection and Cybercrime is based on. As such, it is essential to note the various measures implemented by the forthcoming General Data Protection Regulation, intended to cull these shortcomings. The latter include; fragmented dispute resolution mechanisms, the deficiency of fundamental rights in data protection law, the bureaucratization of data protection law and the immense need for reference to privacy in data protection.

The European Commission has published the following principles to act as overarching guidelines in the drafting of the data protection regulations: these are the principles of subsidiarity and proportionality<sup>270</sup>, as well as the protection of fundamental rights in data usage<sup>271</sup>,

### **THE LEGAL PRINCIPLES GUIDING THE DRAFTING OF THE GENERAL DATA PROTECTION REGULATIONS:**

The drafting of the Regulations and the determination of their scope and applicability are firmly founded upon the following legal principles:

- 1. Subsidiarity and proportionality.**
- 2. The protection of fundamental rights in data usage.**

#### **1. Subsidiarity & Proportionality:**

According to the principle of subsidiarity (Article 5(3) TEU), action at the larger Union level shall be taken only if and in so far as the objectives envisaged cannot be achieved sufficiently by Member States, but can rather, by reason of the scale or effects of the proposed action, be better

---

<sup>270</sup> Proposal for Regulation of The European Parliament and of The Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), p.5

<sup>271</sup> Proposal for Regulation of The European Parliament and of The Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), p.5



achieved by the Union. An apt analysis of the principle of subsidiarity indicates the necessity of EU-level action, which can be justified by the following grounds<sup>272</sup>.

The right to the protection of personal data, enshrined in Article 8 of the Charter of Fundamental Rights, requires the same level of data protection throughout the Union. The absence of common rules creates the risk of different levels of protection in the Member States and create restrictions on cross-border flows of personal data between Member States with different standards.<sup>273</sup>

Personal data are transferred across national boundaries, both internal and external borders, at rapidly increasing rates. In addition, there are practical challenges to enforcing data protection legislation and a need for co-operation between Member States and their authorities, which needs to be organized at a larger level to ensure unity of application of Union law.<sup>274</sup> The African Union is also best placed to ensure effectively and consistently the same level of protection for individuals when their personal data are transferred to third countries.

The European Union noted that its Member States could not alone reduce the problems in the current data protection regime, particularly those due to the fragmentation in national legislations.<sup>275</sup> Thus, there exists a specific need to establish a harmonized and coherent framework allowing for a smooth transfer of personal data across borders within the EU while ensuring effective protection for all individuals across the EU. In a similar vein, with the proliferation of data usage across the African continent, there is a need for the unified effort of States to guarantee the data integrity of various states.

---

<sup>272</sup> Proposal for Regulation of The European Parliament and of The Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), p.15

<sup>273</sup> Proposal for Regulation of The European Parliament and of The Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), p.15

<sup>274</sup> Proposal for Regulation of The European Parliament and of The Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), p.15

<sup>275</sup> Proposal for Regulation of The European Parliament and of The Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), p.17



Legislative actions undertaken by the larger Union will be more effective than similar actions at the level of Member States because of the nature and scale of the problems, which are not confined to the level of one or several Member States.<sup>276</sup>

It is crucial to note that the principle of proportionality requires that any intervention is targeted and does not go beyond what is necessary to achieve the objectives. This principle has guided the preparation of the proposal from the identification and evaluation of alternative policy options to the drafting of the legislative proposal.<sup>277</sup>

## **2. The protection of fundamental rights in data usage:**

The right to protection of personal data is established by Article 8 of the Charter and Article 16 TFEU and in Article 8 of the ECHR. As underlined by the Court of Justice of the EU<sup>278</sup>, the right to the protection of personal data is not an absolute right, but must be considered in relation to its function in society<sup>279</sup>. Data protection is closely linked to respect for private and family life protected by Article 7 of the Charter. This is reflected by Article 1(1) of Directive 95/46/EC which provides that Member States shall protect fundamental rights and freedoms of natural persons and in particular their right to privacy with respect of the processing of personal data.

Other potentially affected fundamental rights enshrined in the Charter are the following: freedom of expression<sup>280</sup>; freedom to conduct a business<sup>281</sup>; the right to property and in particular the protection of intellectual property<sup>282</sup>; the prohibition of any discrimination amongst others on

---

<sup>276</sup> Proposal for Regulation of The European Parliament and of The Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), p.17

<sup>277</sup> Proposal for Regulation of The European Parliament and of The Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), p.18

<sup>278</sup> Court of Justice of the EU, judgment of 9.11.2010, Joined Cases C-92/09 and C-93/09 Volker und Markus Schecke and Eifert [2010] ECR I-0000.

<sup>279</sup> In line with Article 52(1) of the Charter, limitations may be imposed on the exercise of the right to data protection as long as the limitations are provided for by law, respect the essence of the right and freedoms and, subject to the principle of proportionality, are necessary and genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others.

<sup>280</sup> Article 11 of the Charter of the Fundamental Rights of the European Union

<sup>281</sup> Article 16 of the Charter of the Fundamental Rights of the European Union.

<sup>282</sup> Article 17(2) of the Charter of the Fundamental Rights of the European Union.



grounds such as race, ethnic origin, genetic features, religion or belief, political opinion or any other opinion, disability or sexual orientation<sup>283</sup>; the rights of the child<sup>284</sup>; the right to a high level of human health care<sup>285</sup>; the right of access to documents<sup>286</sup>; the right to an effective remedy and a fair trial<sup>287</sup>.

The incorporation of the protection of fundamental rights within the AU data protection regime is imperative to the adoption of data protection measures within Member States' local jurisdictions. The effect of such integration into local statutes is the improved enforceability of Union data protection tenets and the prioritization of fundamental rights in software design, creation and sale within the African digital market.

### **B. Conclusion:**

The need for systematized data protection regulation is evident in Africa, and as the number of cloud technologies grow, the ill-preparedness of African policymakers will continue to be a thorn in the flesh for the development of multinational enterprises from their jurisdictions. Further, inadequate data export restrictions may lead to their citizens' fundamental rights being violated for the benefit of economic success. The news however is not all that bleak. Currently, 14 African countries have privacy framework laws and some sort of data protection authorities in place. Once the African Union Convention on Cyber Security and Personal data Protection (Convention) is ratified across the continent, many other nations will likely enact personal data protection laws. Moreover, as of 1/1/2016, seven African countries have data protection bills in place: Kenya, Madagascar, Mali, Niger, Nigeria, Tanzania, and Uganda. In addition, many analysts believe that the Convention seeks to replicate the European Union data protection model whereby each country has its own national data protection laws and authority. This evidences that, African legislators are not oblivious of the threat that inadequate data protection legislation poses, and the drafting of the Convention and its continued ratification and adoption continues to spur positive growth in the data protection regime.

---

<sup>283</sup> Article 21 of the Charter of Fundamental Rights of the European Union.

<sup>284</sup> Article 28 of the Charter of the Fundamental Rights of the European Union.

<sup>285</sup> Article 35 of the Charter of the Fundamental Rights of the European Union.

<sup>286</sup> Article 42 of the Charter of the Fundamental Rights of the European Union.

<sup>287</sup> Article 47 of the Charter of the Fundamental Rights of the European Union.



Kenya, as the market leader in information technology products and services in Sub Saharan Africa has a significant role to play in the integration of data protection in Africa's future. The experiences brought by the creation of numerous cloud-based technologies within her jurisdiction has put Kenyans on a pedestal as this market experience has enabled Kenyan policy makers to develop more effective data protection strategies than her counterparts. The latter can also be justified by the superior digital market, wherein the use of software products is customary, market behaviours can easily be determined and harmful trends can be determined and legislated against. The impending Data Protection Bill and the African Union's Convention on Personal Data Protection and Cybercrime may be our nation's first step towards unleashing the immense potential our nation has always possessed.

In conclusion, according to the constitutional principles asserted by the Justice Lenaola I. in the case of *Benard Murage v. Fineserve Kenya & 4 others*, the seeds of data protection regulation in our nation can be based upon the rich constitutional tenets of privacy and consumer rights, whose apt implementation within the emergent data protection regime could ultimately protect citizens from the hazards of the bureaucratisation of data protection. The latter topic, as the Kenyan jurisdiction is heavily invested in mobile technologies could be an interesting point for further study, as the relationship between national data protection agencies and private mobile number operators will determine the level of penetration and implementation on data protection regulations outlined by the African Union, particularly within the cloud and other emergent technologies.



**BIBLIOGRAPHY:**

**BOOKS:**

1. Millard Christopher; *Cloud Computing Law*, Oxford University Press, Great Clarendon Street, Oxford , United Kingdom, 2013.
2. Lloyd J. Ian, *Information Technology Law, Sixth Edition* published in Oxford University Press, Great Clarendon Street, United Kingdom, 2012.
3. Carey Peter with Bridget Treacy, *Data Protection (A practical guide to the United Kingdom and European Union Law)*, Oxford University Press, Great Clarendon Street, United Kingdom, 2012.
4. Carey Peter, *Data Protection Handbook*, Oxford University Press, Great Clarendon Street, United Kingdom, 2012.
5. Kuner Christopher, *Transborder Data Flows and Data Privacy Law*. Oxford University Press, Great Clarendon Street, United Kingdom, 2013.

**JOURNAL ARTICLES**

1. Kuan Hon and Christopher Millard, *Cloud Computing vs. Traditional Outsourcing-Key Differences*, Social Sciences Research Network (12/9/2012)
2. Simitis, 'Reviewing Privacy in an Information Society', University of Pennsylvania Law Rev, Vol. 135, No. 3 (March, 1987)
3. 'The Census Decision', Human Rights Law Journal 5 (1984).
4. Datenschutzgesetz 2000.
5. *Opinion 05/2012 on Cloud Computing*, Article 29 Data Protection Working Party, WP136
6. Legal Guidance, para. 3.1.7.7. Available at [http://www.ico.gov.uk/upload/documents/library/data\\_protection/detailed\\_specialist\\_guides/data\\_protection\\_act\\_legal\\_guidance.pdf](http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/data_protection_act_legal_guidance.pdf)

**WEB SOURCES:**

1. <http://webcache.googleusercontent.com/search?q=cache:http://www.laits.utexas.edu/~norman/BUS.FOR/course.mat/Alex> (University of Austin)
2. John Chambers' final key note address in Cisco Live 2015, asserted the numerous points made in this paragraph. See video link as attached here. <http://www.youtube.com/watch?v=ujBLqLFNr0s>
3. <http://www.vodafone.com/business/global-enterprise/invisible-infrastructure-the-rise-of-africas-mobile-middle-class-2013-08-22> (Accessed on 5/11/2015)
4. <http://www.theguardian.com/technology/2011/jul/24/mobile-phones-africa-microfinance-farming>
5. [http://www.cisco.com/en/US/solutions/collateral/ns340/ns517/ns224/state\\_of\\_alaska\\_cs.pdf](http://www.cisco.com/en/US/solutions/collateral/ns340/ns517/ns224/state_of_alaska_cs.pdf)





6. See <http://gigaom.com/cloud/more-than-100-sites-went-down-with-ec2-including-your-paas-provider>
7. <http://www.macdonald.com/history/the-first-European-outlet>
8. <http://news.bbc.co.uk/1/hi/technology/6994776.stm>
9. [http://www.coe.int/t/dghl/standardsetting/dataprotection/Legal\\_instruments\\_en.asp](http://www.coe.int/t/dghl/standardsetting/dataprotection/Legal_instruments_en.asp)
10. [http://www.oecd.org/pages/0,3417,en\\_36734052\\_36761800\\_1\\_1\\_1\\_1\\_1,00.html](http://www.oecd.org/pages/0,3417,en_36734052_36761800_1_1_1_1_1,00.html)
11. <http://www.bakercyberlawcentre.org/appcc/members.htm>
12. <http://www.unhcr.org/refworld/publisher,UNGA,THEMGUIDE,,3ddcafaac,0.htm>
13. <http://www.privacyconference2009.org/home/index-iden-idweb.html>
14. [http://www.theregister.co.uk/2010/01/20/un\\_terror/](http://www.theregister.co.uk/2010/01/20/un_terror/)
15. [http://ec.europa.eu/justice/policies/privacy/lawreport/index\\_en.htm#firstreport](http://ec.europa.eu/justice/policies/privacy/lawreport/index_en.htm#firstreport)
16. See <https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/african-union-convention-cyber-security-and-personal-data-protection-0>
17. [http://ec.europa.eu/justice\\_home/fsj/privacy/docs/wpdocs/2007/wp136\\_en.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf)
18. <http://www.itspublicknowledge.info/applicationsanddecisions/Decisions/2005/200500298.asp>
19. See <http://news.bbc.co.uk/1/hi/technology/4630694.stm>
20. <http://news.electricalchemistry.net/2009/10/cracking-passwords-in-cloud.html>
21. [http://www.ico.gov.uk/upload/documents/library/data\\_protection/detailed\\_specialist\\_guides/data\\_protection\\_act\\_legal\\_guidance.pdf](http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/data_protection_act_legal_guidance.pdf)
22. <http://www.B4U.com>

1. LEGISLATION:

1. The United Kingdom Data Protection Act (1998)
2. The European Union Data Protection Directive (Directive 95/46/EC)
3. The Constitution of Kenya (2010)
4. The Consumer Protection Act (2012), Act No. 46 of 2012.)



5. The Kenya Information and Communications Act, Chapter 411A, (1998) Revised Edition (2012)
6. The Central Bank of Kenya Act, Chapter 491, (2012), Revised Edition (2014)

**2. TREATIES AND CONVENTIONS:**

1. The Council of Europe's Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data, Reference No. CETS No.108.
2. Charter of the Fundamental Rights of The European Union (2000/C 364/01)
3. The Organisation of Economic Cooperation and Development (OECD) Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013), [C(80)58/FINAL, as amended on 11 July 2013 by C(2013)79].
4. The United Nations Guidelines for the Regulation of Computerized Personal Data Files, Adopted by General Assembly resolution 45/95 of 14 December 1990
5. The African Union Convention on Cybersecurity and Personal Data Protection, EX.CL/846(XXV)