Data Colonialism: The New Frontier in Corporate Governance and the 'Corporations and Human Rights' Discourse.

Lois M. Musikali*

Abstract

This paper provides an overview of corporate governance scholarship from inception to-date and situates the current issue of managing Big Data within corporate governance practice and scholarship. Its aim is to highlight the possible impact of Big Data on current corporate governance practice and regulation with a view to encouraging further research on the same. Whilst digitisation has aided advances in good corporate governance practice and regulation, the effects of digitisation have not all been positive: a significant number of corporate governance scandals today are digital. With a focus on data mining, this paper explores this phenomenon, Africa's readiness for it and the surrounding issues it raises both within corporate governance and human rights. That Big Corporations are able to mine data without the data subjects knowledge and use it to their advantage without the data subject's informed consent and compensation has resulted in a phenomenon referred to as 'data colonialism'. This paper evaluates the extent to which Africa and in particular Kenya is prepared for the current world of data harvesting and assesses the need for effective data mining regulation in Africa. It considers the effect of the General Data Protection Regulation (GDPR) on Kenya's Data Protection Act and questions whether Kenya's legal framework can effectively deal with data mining while highlighting the role that corporate governance has in improving accountability in the way Big Corporations handle data.

* Lois M. Musikali is an Advocate of the High Court of Kenya and currently a Senior Lecturer at the Daystar University, School of Law. Her expertise is in the area of corporate governance with her general research interests being in the area of commercial law. The views in this paper and any errors therein are, of course, her own.

Introduction

Ignited by the need to provide a solution to corporate governance scandals around the US and Europe such as the Maxwell scandal of 1991, the Barings Scandal of 1995, the Enron scandal of 2002, and the Parmalat scandal of 2003, corporate governance scholarship began by focussing on understanding the main issues that arise in relation to the governance of public limited companies. The main concern has been that due to a separation of ownership and control, regulation is necessary to ensure that those in control – management - act in the owners' interests. Corporate governance scandals have not just been a preserve for the developed world. The developing world has also had its fair share of scandals. In particular, Kenya has had its fair of corporate governance scandals including the Eurobank scandal of 1993, the Charterhouse Bank scandal of 2004, Uchumi scandal of 2006, the Discount Securities scandal of 2008, Nyaga stockbroker's scandal of 2008, the CMC board-room war of 2011, the East African Portland boardroom wars that started in 2012, the Nakumatt Holdings scandal of 2018, the National Youth Service Scandal of 2018, and the Mega-dams scandal of 2019 amongst others. In all these scandals, a lot of money, some of which belonged to stockholders and pension funds, jobs as well as market confidence and global competitiveness has been lost. Given the diversity of sectors in which corporate governance scandals have played out, recent scholarship has expanded into other sectors such as state corporations, insurance, bank and cooperative sectors, as well as family companies.

In particular, the aim has been to develop corporate governance systems that can respond to internal governance issues. Amongst the issues that have been of interest to corporate governance have included core theories of corporate governance, for example, the principal-agent problems between directors and shareholders, and between minority and majority shareholders; the proper objective of the corporation – should it be shareholder wealth maximisation, or consideration, or prioritisation of stakeholder concerns, such as employee protection or industrial democracy, as well as the consideration of the importance of maintaining supplier relationships, and therefore the important role of trust and relational contracting, how to regulate directors – should countries adopt a

hard or soft law approach, understanding the role of market controls such as the labour market, capital markets and takeover markets, the role of internal voice - be it non-executive directors or shareholder activism - and the appropriate level of directors' remuneration. In an effort to understand these issues, corporate governance scholarship has taken a comparative focus, the aim being to assess the principal forms of corporate governance, control and regulation of the firm across countries. In particular, the legal relationship between directors, managers, and shareholders. More recently, the focal point has been to analyse the growing empirical research on comparative corporate governance with a view to providing a theoretical and practical grasp of core issues of corporate governance, which can be useful for academic as well as professional work in this field. In this regard, the role of international organisations such as the Organisation for Economic Co-operation and Development (OECD) and the World Bank has been considered.

Corporate governance scholarship has not only focused internally within the corporation but also on the external effects that corporations have had on society. Corporations can have an impact on human rights through their relationships with their employees, consumers, communities around them and also through their supply chain relationships. The activities of corporations may harm the communities in which they exist, such as the Ukraine's Chernobyl nuclear disaster of 1986 in which a nuclear accident killed 31 people and left uncountable people affected for the rest of their lives. Corporations may have a supplier that employs forced labour or child labour practices for instance the Nike scandal of 2002, in which Nike was accused of using sweatshops[1] since the 1970s to produce footwear and apparel. Corporations may be polluting the environment and this may be affecting the health or livelihood of people around the world. A recent example is the Volkswagen emission scandal of 2015 in which Volkswagen had intentionally programmed turbocharged direct injection diesel engines to activate their emissions controls only during laboratory emissions testing which causes the vehicles 'no' output

[1] Sweatshop or sweat factory is a term that refers to a workplace with very poor, socially unacceptable or illegal working conditions.

to meet US standards during regulatory testing, but emit 40 times more in real-world driving. This software was installed in 11 million Volkswagen cars worldwide between 2009 and 2015. A similar scenario played out in the Nissan 2020 scandal where it was discovered that some emissions and fuel economy tests on Nissan cars sold in Japan had deviated from the prescribed testing environment. As was the case in the 2015 Volkswagen scandal, defeating devices had been installed and inspection reports altered.

This has resulted in calls for corporate social responsibility in the international business arena. Debates on the role of international organisations in promoting business compliance with human rights and environmental norms have been examined. Corporations as international actors, the idea of international civil society, as well as state responsibility for the acts of corporations that violate international norms on human rights and the environment have been of academic interest. In this regard, the role of international organisations in promoting or enforcing corporate social responsibility, the OECD and the International Labour Organisation (ILO), European Union policies on corporate social responsibility, The UN Global Compact amongst others have been considered.

A lacuna has remained on how the corporation is to engage with the rapid digitisation of today's world. Early attempts to engage with digitisation in corporate governance scholarship took the form of incorporating knowledge management and information communication technology (ICT) into policy-making. Corporate governance in this regard sought to highlight the importance of information and communication technology, how information technology (IT) drives business, its competitive advantage and how boards can attract and retain skilled technology personnel in organisations. Corporate governance scholarship further outlined how IT is facilitating team-work, creativity and innovation with critical issues such as access to information, the internet, intranet, ICT security, ICT policy, strategy and evaluation of an organisation's ICT system. The effects of digitisation have not all been positive for individuals and corporations. Digitisation has come with its fair share of scandals such as the Edward Snowden scandal and Facebook's Cambridge Analytica

scandal, which some have felt are human rights violations, particularly a violation to the right of privacy, prompting the need for scholarship in this area. Most recently there has been a call towards creating the role of Data Commissioner as well as adopting and cementing the role of the Corporate Information Officer (CIO) in corporations by making it a recommendation in corporate governance codes. Notable, in Kenya, in this regard is the recent creation of the position of Data Commissioner and the impact that this position is likely to have.[2] However, it remains questionable whether boards understand the digital environment in which companies now exist, and in effect the CIO is working in to be able to get the most out of the CIO. Of particular interest is a trend in today's world known as data mining.

The Concept of Data Mining

Today's world is characterised by the existence of big companies such as Alibaba, Amazon, Apple, Facebook, Google and Microsoft. All of them are big tech with algorithms at their core.[3] These companies have now countered the dominance of energy giants, the so called 'big oil' such as BP, Exxon Mobil, PetroChina and Royal Dutch Shell at the top of stock market indexes. Data is 'the new oil'.[4] It is speculated that it is now impossible to live and function day-to-day in the digital world outside the ecosystem created by these big tech companies. We are in the midst of a great race for data in which we are more than just customers of these businesses. We are generators of data which can then be converted to 'big data.' 'Big data' refers to data which emerges as a commodity when individual datums by the million, billion or more, are linked together algorithmically.[5] Big tech companies need us to like them to become indispensable as the more we use them, the more data we produce. To 'big tech' companies as data vendors, the purpose of 'big data' is to transform unpredictable individual

[2] Ayega, Davis, Kassait to be Sworn In as Data Commissioner after House Approval, Capital News, November 6, 2020.

[3] Al Jazeera English, Is Big Tech Colonising the Internet?: All Hail the Algorithm (2019).

[4] Couldry, Nick, Mejias, Ulises and Oswego, Suny (2018), 'Data Colonialism: Rethinking Big Data's relation to the Contemporary Subject, Television and New Media.

[5] Thatcher, Jim, O'Sullivan, David and Mahmoudi, Dillion (2016) 'Data Colonialism through Accumulation by Dispossession: New Metaphors for Daily Data', Environment and Planning D-Society & Space, 34 (6).

consumers into predictable statistical aggregates of consumption.[6] It is all about the data for these businesses: how much data can they get about people so that they can sell 'ads' and create predictive things to keep people hooked on what they are able to offer. This phenomenon has been identified by Thatcher et al who state that the aim of users of 'big data' is not simply to store and retrieve large datasets for their own sake, but to gain knowledge from them via analysis – in order to enhance decision making in the pursuit of efficiencies and profit.[7] How can individuals and corporations ensure that their data is not being stolen and misused?

Data mining in its traditional form is not a new issue. Perhaps we are more versed with it being referred to as data collection. Traditionally, social knowledge was produced through data collection, a method forged in the nineteenth century. Nation states would gather public statistics through survey questions answered by human beings and interpreted by human beings. As a mode of social knowledge, it had the following features which are not shared by 'big data.' First, it was publicly funded and collected in most countries through the census. Secondly, it was publicly analysed and put to use by governments and by civil society organisations that wanted social reform. Thirdly, this knowledge was publicly debated.[8] Social policy until twenty years ago or so was shaped by public knowledge. Commercial corporations in the nineteenth century were beginning to establish themselves as institutions. At that time, they were the buyer, not the seller of this social knowledge. They depended on the government to share social knowledge. This traditional model of social knowledge was transparent and accountable. The statistical models used were simple and as a result those disadvantaged by them could challenge them. Today's emerging model of social knowledge is based on pools of big data, processed by huge banks of parallel computers using machine learning. This new way of collecting social knowledge is privately collected[9] and funded, privately analysed and privately debated in corporations.

[6] Ascher (2016) cited in Thatcher, Jim, O'Sullivan, David and Mahmoudi, Dillion (n 5).

[7] Thatcher, Jim, O'Sullivan, David and Mahmoudi, Dillion (n 5).

[8] Nick Couldry, Making Sense of the Digital Economy, Colonised by Data. 20th November 2018, Auditorium Friedrichstrasse, Berlin.

[9] See Thatcher, Jim, O'Sullivan, David and Mahmoudi, Dillion (n 5).

Little, if any, regard is given to privacy in the collection of this data. As Thatcher *et al* put it, previously private times and places are commodified and privatised as a new terrain for capital investment and exchange.[10] Due to the extreme complexity and massive repetition upon which machine learning depends, this knowledge and its processes are largely opaque.[11] The remoteness of this new social knowledge from daily understandings of the world has been noted in an article in Forbes Magazine which stated that Uber's CEO Travis Kalanick showed attendees at Uber's Chicago Launch party a city's Uber heat map in September 2011 *via* Uber's Facebook page. Generally, each launch of a black car and ride-sharing service was marked with a lavish launch party to which the local tech glitterati were invited. One of the go-to Uber party tricks for the events was to treat attendees to Uber's "God-View," which lets them see all of the Ubers in a city and the silhouettes of waiting Uber users who have flagged cars. This is not an issue when it is anonymous. However, an attendee at a launch party says Uber treated guests to a Creepy Stalker View, showing them the whereabouts and movements of 30 Uber users in New York in real time. She recognised half of the people listed and texted one of them revealing that she knew his current whereabouts, much to his displeasure.[12]

Another feature of today's algorithmic social knowledge is that it is not based on talking to people, asking what they think, how they reflect, how they interpret the world they share as was the case with statistics. Instead the goal of artificial intelligence and therefore its huge attraction for corporations and governments, with the relevant computer capability, is the finding of proxies. Proxies discovered after countless layers of pattern seeking emerge as a good enough substitute for predicting when two things will be correlated.[13] Finally, ethical guidelines were a key feature of traditional data collection. Ethical guidelines were intended to help statistics practitioners make decisions ethically and to promote

[10] Thatcher, Jim, O'Sullivan, David and Mahmoudi, Dillion (n 5).

[11] Nick Couldry (n 8).

[12] Kashmir Hill, 'God View': Uber Alledgedly Stalked Users For Party-Goers' Viewing Pleasure (Updated), Forbes, October 3, 2014.

[13] Nick Couldry (n 8).

accountability by informing those who rely on statistics analysis of the standards they should expect. Traditional statistical practice was fundamentally based on transparent assumptions, reproducible results, and valid interpretations with stakeholders being expected to act in good faith.[14] The issue of ethics is hardly mentioned in data mining as the giver of the data hardly has any idea that the data in question is being collected. The raising of concerns about data mining has more often than not been met with a wet blanket.

Data Mining and Data Colonialism

The revelations of Edward Snowden, an American whistleblower, in 2013 showed us that something big is going on with data. Snowden, who was hired by a National Security Agency (NSA) contractor, gradually became disillusioned with the programs with which he was involved and tried to raise his ethical concerns through internal channels but was ignored. Snowden copied and leaked highly classified information from the NSA in 2013 when he was a Central Intelligence Agency (CIA) contractor.[15] The real story in those revelations was how much data corporations were already collecting from people, from which governments simply sought to benefit. Snowden's disclosures revealed numerous global surveillance programs, run by NSA and the Five Eyes Intelligence Alliance (FVEY) with the cooperation of telecommunication companies and European governments.[16] FVEY, an alliance between the US, UK, Canada, Australia and New Zealand, is the most enduring multilateral intelligence sharing network, having been formed in 1947. FVEY focuses on collecting and sharing signals intelligence. The key players in FVEY are the US and the UK with the other countries maintaining junior positions to them, being mainly consumers rather than producers of intelligence. These other countries are still important as Australia, for example, provides FVEY with intelligence in relation to South-East Asia and the Pacific region.[17]

[14] ASA, Ethical Guidelines for Statistical Practice, prepared by the Committee on Professional Ethics of the American Statistical Association 2018.

[15] BBC News, Edward Snowden: Leaks that exposed US spy programme, January 17, 2014.

[16] Business, Who holds security clearances, The Washington Post, June 10, 2013.

[17] Monique, Mann and Daly, Angela (2019), '(Big) data and the north-in-south: Australia's Informal Imperialism and digital colonialism,' Television and New Media, 20 (4), pp.379-395.

Snowden's revelations showed that US and British intelligence agencies had successfully cracked much of the online encryption relied on to protect the privacy of personal data, online transactions and emails.[18] NSA and its UK counterpart Government Communications Headquarters (GCHQ) had broadly compromised the guarantees that internet companies have given consumers to reassure them that their communications, online banking and medical records would be indecipherable to criminals and governments.[19] NSA and GCHQ insisted that the ability to defeat encryption is vital to their core missions of counter-terrorism and foreign intelligence gathering.[20] These revelations prompted a discussion about national security and individual privacy with security experts accusing NSQ and GCHQ of attacking the internet itself and the privacy of all users as cryptography forms the basis of trust online.[21]

Another scandal that would reveal the extent of data mining is the Facebook-Cambridge Analytica scandal of 2018 where Cambridge Analytica harvested the personal data of millions of people's Facebook profiles without their consent and used it for political advertising. The Facebook-Cambridge Analytica scandal prompted many to check what data was being collected about them by platforms such as Facebook and through search engines such as Google. This scandal began with Aleksandr Kogan, a data scientist at Cambridge University, being hired by Cambridge Analytica to develop an app called, 'This is Your Digital Life.'[22] Kogan provided the app to Cambridge Analytica[23] and Cambridge Analytica arranged an informed consent process for research in which several hundred thousand Facebook users would agree to complete a survey

[18] Ball, James, Borger, Julian and Greenwald, Glenn, Revealed: How US and UK spy agencies defeat internet privacy and security, The Guardian, September 6, 2013.

[19] Ball, James, Borger, Julian and Greenwald, Glenn (n 18).

[20] Ball, James, Borger, Julian and Greenwald, Glenn (n 18).

[21] Bruce Schneier, an Encryption Specialist and Fellow at Harvard's Berkman Center for Internet and Society, quoted in Ball, James, Borger, Julian and Greenwald, Glenn (n 18).

[22] Hern, Alex, How to Check whether Facebook shared your Data with Cambridge Analytica, The Guardian, April 10, 2018.

[23] Graham–Harrison, Emma, Cadwalladr, Carole, Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach, The Guardian, March 17, 2018.

that was for academic use in exchange for payment.[24] Facebook however, allowed this app to not only collect personal information from survey respondents but also from the respondents' Facebook friends resulting in Cambridge Analytica acquiring data from millions of Facebook users.[25] The Facebook-Cambridge Analytica scandal erupted in 2018 with an ex-Cambridge Analytica employee, Christopher Wylie being the whistle-blower.[26]

Christopher Wylie has stated that Cambridge Analytica is an example of modern day colonialism having expanded its operations to developing countries such as Mexico, Malaysia, Brazil and Kenya and having worked extensively in India.[27] Citing Cambridge Analytica's work in Kenya's presidential campaign of 2017, Wylie stated that, "This is a company that goes around the world and undermines civic institutions of... countries that are struggling to develop these institutions. ..They are an example of what modern day colonialism looks like. You have a wealthy company from a developed nation going into an economy or democracy that is still struggling to get... its feet on the ground and taking advantage of that to profit from that."[28] This issue of profit has been flagged by Thatcher *et al* who point out that this epistemological orientation towards the relentless pursuit of 'bigger' data is driven by intense profit-seeking competition within capitalist markets and industries.[29] Cambridge Analytica is alleged to have used data gathered from Facebook users via a third party app to influence votes, including the US presidential election and the Brexit referendum of 2016.[30]

[24] Cadwalladr, Carole, The Great British Brexit Robbery: How our Democracy was Hijacked, The Guardian, May 7, 2017.

[25] Graham–Harrison, Emma and Cadwalladr, Carole (n.23).

[26] Larsen, Karin, Who is Christopher Wylie? How a B. C. High School Dropout set out on path to Political Data Harvesting, CBC News, 20th March 2018.

[27] Justina Crabtree, Cambridge Analytica is an 'example of what modern day colonialism looks like,' whistleblower says, CNBC, March 27, 2018.

[28] Justina Crabtree (n 27).

[29] Thatcher, Jim, O'Sullivan, David and Mahmoudi, Dillion (n 5).

[30] Justina Crabtree (n 27).

The race for data has resulted in a phenomenon that is referred to as 'data colonialism.'[31] Data colonialism, unlike traditional colonialism is in its early stages – it has been around for about twenty years now. Under this phenomenon, traditional colonialism's four underlying functions of extraction and appropriation of resource, empire building through the creation of new social relations to stabilise that appropriation, the extreme concentration of wealth that flowed from that appropriation and the ideology that was used to tell a different story of what was going on, most notoriously the ideology of civilisation can be seen. These same four levels are at work in data colonialism.[32] First, there is the appropriation of resources itself. Couldry et al state that data colonialism combines the predatory extractive practices of historical colonialism with the abstract quantification methods of computing.[33] Human life, human experience and action become a direct input to capital.[34] Social life all over the globe has become an 'open' resource for extraction that is somehow 'just there' for capital.[35] The idea is that it is just worthless human 'exhaust' that is taken. According to Couldry *et al* a blurring of the links of data back to a prior process of data collection is achieved through the common idea that data are 'merely' the 'exhaust' exuded by people's lives, and so not capable of being owned by anyone.[36] Perceiving data as something that is naturally there anyway for the taking, conveniently forgets all the mechanisms that are needed to gather, format, extract and process this supposedly natural resource. Data colonialism is therefore not just about extraction: it is also about appropriation. Appropriation happens when data about one individual's actions or properties at one moment is combined with data about other actions, moments and properties to generate valuable relations between data points.[37]

[31] Data colonialism as a metaphor to describe the process of accumulating 'big data' was suggested by Thatcher *et al* in Thatcher, Jim, O'Sullivan, David and Mahmoudi, Dillion (n 5).

[32] Nick Couldry (n 8).

[33] Couldry, Nick and others (n 4).

[34] See Couldry, Nick and others (n 4).

[35] Couldry, Nick and others (n 4).

[36] Couldry, Nick and others (n 4).

[37] Couldry, Nick and others (n 4).

Secondly, social relations are being colonised by data processes as all social relations increasingly take the form of 'data relations' that maximise data extraction for value. The phrase 'data relations' refers to new types of human relations which enable the extraction of data for commodification. Under these new types of human relations, social life all over the globe becomes an 'open' resource for extraction that is somehow 'just there' for capital.[38] Third, the economic value that is extracted is hugely concentrated in the vast wealth of new colonial corporations which is referred to as the 'social quantification sector' (SQS): Facebook, Google, Amazon, Apple, Baidu, Alibaba, China's Tencent and so on.[39] Corporations are the main actors in the SQS: they capture everyday social acts and translate them into quantifiable data which is analysed and used for the generation of profit. According to Couldry *et al*, the SQS includes both big and small hardware and software manufacturers, developers of social media platforms, and firms dedicated to analysis and brokerage. The firms dedicated to analysis and brokerage are a largely unregulated part of the economy, specialising in collecting information from medical, finance, criminal and other records for categorising individuals through algorithmic means. These data brokers package and sell those lists to advertisers and other users such as governments and law enforcement agencies.[40] Finally, there are new colonial ideologies that seek to disguise what is going on. Not the idea of civilisation exactly yet, but the idea that we must always stay connected. That everything must be put into data form so that, for example, we can get more personalised messages and products and the idea that all of this, including the tracking is somehow inevitable. All four dimensions of traditional colonialism are at work in our life with data today.[41] These similarities between traditional colonialism and data colonialism have been noted by Thatcher et al who observe that the processes by which data is transformed into commodity occur through asymmetrical relations

[38]Couldry, Nick and others (n 4).

[39]Couldry, Nick and others (n 4).

[40]Couldry, Nick and others (n 4).

[41]Nick Couldry (n 8).

between data producers - end-users -, and data collectors and owners - corporate entities - that mirror processes of primitive accumulation or accumulation by dispossession.[42]

As Couldry puts it, there is a new land grab going on. It is not land that is being grabbed, it is us: it is the grabbing of valuable data out of our lives.[43] Our data is with us, ready to be extracted, just as oil can be extracted from the earth. Data colonialism, unlike traditional colonialism, does not involve horrific violence and for this reason, we may not realise it is happening. The reason for this is that unlike traditional colonialism which represents the physical presence of a colonial power in a given geographical place, digital colonialism involves the dissemination of information and highly classified surveillance to and from remote destinations as a means of perpetuating traditional colonial discourses via technological innovation.[44] An instance is whenever we interact with the terms of service of an end-user licence agreement when we are signing up for an app or a new social media platform. Usually, there is an often long small print document called 'Terms of Service' asking us to agree to something that we often do not even understand. Couldry et al have described the contents of Terms of Service documents as containing, 'outlandish appropriative claims by corporations.'[45] In normal instances, no one reads the terms. We just click 'I accept' because we want to get on and get the pleasurable experience of using the app or the platform. As Pariser put it individuals are offered notional advantages – pleasurable experiences in which aspects of their lives are algorithmically sorted and produced for them based on their quantified markers, for example, the offering of nearby restaurants and bars - based on previous inputs - by apps such as Foursquare City Guide.[46] Sometimes our acceptance is just assumed: no questions asked.[47] By that

[42] Thatcher, Jim, O'Sullivan, David and Mahmoudi, Dillion (n 5).

[43] See Nick Couldry and Ulises Mejias, *The Costs of Connection: How Data is Colonizing Human Life and Appropriating it for Capitalism* (Stanford University Press, 2019).

[44] Monique, Mann and Daly, Angela (n 17).

[45] Couldry, Nick and others (n 4).

[46] Pariser (2011) cited in Thatcher, Jim, O'Sullivan, David and Mahmoudi, Dillion (n 5).

[47] The GDPR has tried to disrupt that assumption.

act of acceptance, express or implied, we enter into a whole set of 'data relations' that unfold in ways we only partly understand. We enter into data relations every day, a habit that is becoming so regular that it does not seem like appropriation much of the time. Rather, it is seen as just convenience. It sometimes seems a mystery how we can accept so much with so little resistance.[48] We end up signing away our rights and property through the act of clicking 'I accept' without realising the extent of what we have given up. Thatcher et al put it this way: as users of technology enter into tacit data license agreements with the firms that create and control the technology, they are dispossessed of the right to control that data they have produced.[49]

Data Harvesting: The New Capitalism

As we have seen, data harvesting has become an everyday feature of daily life. Data harvesting is not just a development or a new phase of capitalism, it is a new phase of colonialism that will in time provide the fuel for a later stage of capitalism whose full shape cannot be predicted yet.[50] According to Thatcher et al, the emergence of big data does not occur in a vacuum but as part of an asymmetric power relationship in which individuals are disposed of the data they generate in their day-to-day lives. The asymmetry of this data capture process is a means of capitalist "accumulation by dispossession" that colonises and commodifies everyday life in ways that were previously impossible.[51]

This new stage of capitalism will not be premised on labour as was the case with traditional capitalism[52] but on data relations, which is why violence may not be a descriptor of data colonialism.[53] Perhaps, then the heart of data colonialism is something so big that it almost escapes us: it

[48] Nick Couldry (n 8).

[49] Thatcher, Jim, O'Sullivan, David and Mahmoudi, Dillion (n 5).

[50] See Couldry, Nick and others (n 4).

[51] Thatcher, Jim, O'Sullivan, David and Mahmoudi, Dillion (n 5).

[52] Foley Duncan and Dumenil Gerard (2008) 'Marx's Analysis of Capitalist Production', The New Palgrave Dictionary of Economics, 2nd Edition, Abstract.

[53] Nick Couldry (n 8).

is the new corporate strategy, the new corporate dream you can hear from every boardroom in most countries that underlies most of the details of datification[54]; the dream of annexing to capital every point in space and time. Of cloning social relations on digital platforms and elsewhere so that this annexation to capital seems just natural and through this building a social order that capitalises human life without any possible limit.[55] The annexation of human life to the forces of capital is a land grab without precedent in human history. This is an annexation, that to be effective does not need violence because an all-encompassing network of social relations is already in place on the foundations of which new forms of data relations can be built provided we 'agree'.[56]

Data Colonialism in Africa

Data colonialism, unlike traditional colonialism is not about the 'West' colonising other parts of the world. This new data colonialism works both externally – on a global scale – and internally in these corporations home countries.[57] As Mann and Daly put it, "The privacy (and other human rights) of everyone within Australia (and also people outside of Australia's geographical borders) are routinely violated by Australian mass surveillance, data collection and use."[58] Another example is Facebook which benefits from data from both their home and host populations. That said, there are two centre's of power in data colonialism today: the United States (US) and China.[59] Whilst we know a lot about big US companies such as Microsoft, Google, Amazon, we do not know as much about the big Chinese Companies. A Chinese company that is having a great impact in African economies is Huawei Technologies. Most Africans will have interacted with Huawei Technologies directly by being a user of their products or indirectly by having seen their products. For Huawei Technologies, Africa

[54]Nick Couldry (n 8).

[55]Nick Couldry (n 8).

[56]Nick Couldry (n 8).

[57]Couldry, Nick and others (n 4).

[58]Monique, Mann and Daly, Angela (n 17).

[59]See Couldry, Nick and others (n 4).

has been one of its biggest telecom markets. Huawei has been building products that are suited to the African market in terms of cost. The cheapest phone that you can get in most African markets, including Kenya, is a Chinese manufactured phone. It has been said that ninety percent of Kenya's electronics market is Chinese.[60] In Nairobi, the dominance of Chinese technology is evident: from telecommunication lines to satellite networks, to phones and the apps in those phones. Transsion Holdings, a Shenzhen-based company for instance, was the No. 1 smartphone company in Africa in 2017.[61] Transsion Holdings sells to about 40% of the mobile market in sub-Saharan Africa: its' phones sell under brandnames such as Tecno, iTel and Infinix. The strategy of Transsion Holdings does not end with offering the consumer the hardware: data-driven apps such as the music streaming service Boomplay and the digitial payment platform PalmPay add to a growing repository of data on African users and can help boost money making opportunities for Transsion Holdings.[62]

This has resulted in a concern about surreptitious data collection using Chinese technology in Africa. China is building relationships with governments and providing infrastructure for surveillance and ICT in Africa.[63] Specifically in this regard is the claim that China 'planted bugs' while building the African Union headquarters in 2012. The alleged hack was discovered five years later in 2017 when IT engineers investigated why the centre's computer servers reached a peak for data activity between midnight and 2am. The IT engineers found that the servers were connected to others in Shanghai, and were transferring information.[64] The African Union HQ building was a 'gift' from the Chinese government to help Africa integrate better and improve their institutional capacity, and at the same time an act aimed at solidifying Sino-African relations.[65] There have

[60] Al Jazeera (n 3). See also Hawkins, Amy, Beijing's Big Brother Tech Needs African Faces, Foreign Policy, July 24, 2018.

[61] Hawkins, Amy (n 60).

[62] Al Jazeera (n 3).

[63] Al Jazeera (n 3).

[64] Aislinn Laing, China 'planted bugs' while building African Union HQ, The Times, February 01, 2018.

[65] Abdi Latif Dahir, China "gifted" the African Union a headquarters building and then allegedly bugged it for state secrets, QUARTZAFRICA.

also been concerns about China exporting facial recognition software to Africa.[66] CloudWalkTechnology, a Guangzhou-based start up signed a deal with the Zimbabwean government to provide a mass facial recognition program. The deal between CloudWalk and the Zimbabwean government will not just cover CCTV cameras. According to a report in the Chinese state newspaper Science and Technology Daily, smart financial systems, airport, railway, bus station security and a national facial database will all be part of the project.[67] There is a whole lot of data that is being taken out from African countries to be kept, handled and used by people who are not necessarily responsible or answerable to African people. The big companies such as Huawei argue that they do not access people's data or sell it. Huawei claims that the only data they are using is just to improve their products such as using artificial intelligence in their smart phones and in their network equipment so that it can improve and be faster.[68] Skeptics question the assertion of these big companies and argue that most big companies do exploit user data in some way.

When we compare digital colonialism to traditional colonialism, it is important to remember that the fundamental objective of both is to make money by imposing one society over another so that the first society can make money off that imposition. China has been investing in Africa for a long time now. Whilst China has not pretended that it is doing anything other than expanding its economic interests, the US has been less clear. China has not used the civilising rhetoric because it has not needed to as it is willing to invest in high-risk economies.[69] Contrast that with the big US companies. Microsoft talks about 'democratising A.I',[70] Facebook talks about being concerned about giving 'connection.' Facebook founder,

[66] Hawkins, Amy (n 60).

[67] Hawkins, Amy (n 60).

[68] Al Jazeera (n 3).

[69] See Hawkins, Amy (n 60).

[70] Microsoft News Center, Democratising AI: For Every Person and Every Organisation, September 26, 2016.

Mark Zuckerberg, for instance has stated that "Connectivity can't just be a privilege for some of the rich and powerful, it needs to be something that everyone shares."[71]

Facebook has made a big push to present itself as a benevolent force to give people online access. Since 2013, Facebook has been leading a giant project called, 'internet.org.' Internet.org is a gateway to the worldwide web for those with poor connectivity. The app that serves as the portal of Facebook's version of the internet is called 'Free Basics.' Free Basics gives free access to Facebook and some extras such as weather forecasts. Free Basics has been launched in at least 60 countries, more than half of them in Africa. The idea is to provide access to select sites without data charges. In effect, it is a stripped down version of the internet that has one very important component: guaranteed connection with Facebook and arguably, guaranteed possibilities of data extraction. This is why despite its slick marketing, not everyone is convinced that this is an entirely selfless exercise.[72] Facebook's Free Basics was banned in India. The sort of power that Facebook has sought to exercise through its Free Basics platform is best understood as a neo-colonial move benefitting from the historic asymmetry between Africa and American capital.[73]

Aside from the Free Basics app, Facebook has many other initiatives across Africa. Facebook's latest push in Kenya is called 'Express Wi-Fi' which also falls under the suite of services that Facebook launched under the internet.org initiative. Facebook has teamed up with local internet service providers to install more than one thousand Express Wi-Fi hotspots.[74] Express Wi-Fi is a standard paid-for Wi-Fi service launched as a 'feel-good' people's internet. In terms of cost, Express Wi-Fi is at the cheaper end of Kenya's fiercely competitive data market offering, for instance 3GB of monthly data for Kenya Shillings Five Hundred ($5). In launching Express

[71] Al Jazeera (n 3).

[72] Al Jazeera (n 3).

[73] Nick Couldry (n 8).

[74] Ochieng' Rapuro, Facebook Deepens Consumer Data Mining in Kenya with Firmware, Business Daily, April 10, 2018.

Wi-Fi, Facebook did not want to get into the internet service provider (ISP) business itself. Instead it offered to supply ISP partners the equipment for their Wi-Fi access points. Each access point costs around Kenya Shillings Twenty Five Thousand ($250) and approximately another Kenya Shillings Twenty Thousand to install ($200). In return for these free access points, the local ISPs permanently brand their Wi-Fi as 'powered by Facebook.'[75] One can therefore sign up as a vendor for Facebook's Express Wi-Fi and get a commission on every data bundle they sell. Customers love Express Wi-Fi as their bundles are cheaper compared to other networks, available and strong. Express Wifi has made web access cheaper for people living in under-served locations.[76] However, it is the software in the access points that has raised concerns that Facebook, through Express Wi-Fi is collecting additional citizen data beyond its users. These concerns stem from the way the Express Wi-Fi access points were sourced. Nearly all of the world's Wi-Fi access points are sourced from one of two market leaders: Microtiq and Ubiquiti, and come with an operating system, referred to as firmware. When Facebook set out to source the equipment for the Express-WiFi access points, it approached Ubiquiti with a proposition to make a purchase on condition that it would be allowed to insert its own software – referred to in industry as 'little black box' into each access point. Facebook did not divulge the nature or purpose of the software it was going to insert and for that reason, Ubiquiti refused to insert it. Facebook then went to Cambrian, a less known supplier, which agreed to insert the black box into the access points. The potential loss of sales then forced Ubiquiti to accept the insertion proposed by Facebook. The insertion of these 'black boxes' into the Express Wi-Fi access points is deeply worrying. It has been speculated that beyond mining data from these Express Wi-Fi access points, there is a possibility that Facebook is acting as a 'middle-point monitor', potentially even de-encrypting and re-encrypting data streams from sources such as Google.[77]

[75] Ochieng' Rapuro (n 74).

[76] Al Jazeera (n 3).

[77] Ochieng' Rapuro (n 74).

Facebook is not the only big company playing the connectivity card in Kenya. In 2018, Alphabet, the parent company whose most famous brand is Google's sister company Loon, signed a deal with Telkom Kenya to, "connect the unconnected using balloons."[78] Loon is a path-breaking project. The idea of Loon is to use high altitude balloons to provide internet connectivity in remote and hard to reach parts of the world. Using Loon, Google's mission is to get Africans who are offline, online in a more affordable way with better content that is relevant. What remains to be seen is what standards of accountability there will be in a deal such as that of Loon. Will it mean that people are only restricted to using Google-affiliated sites? What data will be collected in the process of connecting people? Google argues that it ensures that it employs user trust by ensuring that users understand what Google is doing with the data that it has on them. Google also ensures that users are able to manage and control the data that it has on its users.[79]

Legal and Governance Concerns about Data Colonialism

While all individuals experience the commodification and dispossession of their data, marginalised persons and groups experience additional or more acute ways in which their data is 'colonised.'[80] Africa being a marginalised continent in regard to development is likely to be more negatively affected by data mining. The legal concern is that there is no way that these tech companies will be able to behave in their home states the way they behave in their host states in the developing world. Facebook, for example, would not be able to roll out a project as big as Free Basics without some kind of check and balance or ethical loop as they have in Africa. In this regard some apps, such as Kaspersky Internet Security for Android, even have different end-user-licence agreements for those in countries the General Data Protection Regulation (GDPR) region and those in countries with weak frameworks. There has been no effort to educate the consumer on what it means to use these products and what giving their data to these apps means for the consumer. No one asks what Africa wants or needs from the internet.

[78] Al Jazeera (n 3).

[79] Al Jazeera (n 3).

[80] Monique, Mann and Daly, Angela (n 17).

Data colonialism in Africa is framed as a civilising mission. According to the founder of Facebook, Mark Zuckerberg, "when people are connected, we can accomplish some pretty amazing things. We can get closer to the people that we care about. We can get access to new jobs, opportunities and ideas."[81] The interpretation of the latter statement, on whose benefit is being spoken of, is left to our imagination. Interestingly, historical colonialism was also framed in terms of bringing progress, something that is good and beneficial for humanity.[82] Africa's participation is expected and Africa is told that it is for its own good. Users are seen to voluntarily and willingly adopt technologies, and end-user-licence-agreements as part of broad social norms.[83] Meanwhile extraction and capturing of data is happening in the background without Africa realising the true consequences. According to Lanier, the reason people click 'yes' is not that they understand what they are doing, but that it is the only viable option other than boycotting a company in general, which is getting harder to do.[84] It is impossible to ignore the huge potential for data mining: Africans are the ones producing the data but not necessarily the ones to gain from it. At stake here are Africa's ideas, dreams, hopes and frustrations being used to sell other things back to Africa. At what point in this process does Africa get its money back?[85]

These concerns point to the asymmetries of the relations between data producers and owners - end-users and app developers - that have become a focal point of value generation in the technology industry.[86] While data producers generate data through the use of technology to perform social activities, corporations extract value through the quantification of the data. The data producer, as a generator of value, is denied access to the

[81] Al Jazeera (n 3).

[82] Nick Couldry (n 8).

[83] Thatcher, Jim, O'Sullivan, David and Mahmoudi, Dillion (n 5).

[84] Lanier (2014) cited in Thatcher, Jim, O'Sullivan, David and Mahmoudi, Dillion (n 5).

[85] Al Jazeera (n 3).

[86] Thatcher, Jim, O'Sullivan, David and Mahmoudi, Dillion (n 5).

commodity form of value produced through its privatisation as property and alienation into the control of the firm. This value is now owned by the corporation. The data producer is alienated and excluded from the final data commodity.[87]

In 2018, Facebook was forced to admit that it had added its own software to the Wi-Fi access points that enabled non-facebook data such as customer names and phone numbers to directly flow to the corporation. Facebook says the purpose of the software is to ensure that the hotspots are functioning well,[88] there is no clarity on how much additional data is being collected and how it is being used. A lot of these companies are not even Kenyan or African. What is a Kenyan citizen supposed to do when an American company uses their data, sells their data, markets their data as a product without their consent, without their ability to intervene and without their ability to appeal to a court system? This is the grey area with these big companies.

This concern has been aired in relation to China's CloudWalkTechnology's investment in Zimbabwe. Some Zimbabweans are concerned about how their data will be used in China. The question is what CloudWalkTechnology will do with Zimbabwean identities. There have been feelings that "It sounds like a spy game."[89] As part of the Zimbabwe deal, data on millions of black faces will be sent to the Chinese CloudWalkTechnology company to help train its AI technology towards identifying people with darker skin tones. The training of AI to work better on black faces is a significant opportunity for CloudWalkTechnology and for Chinese AI in general. What is notable is that Zimbabweans did not consent to the use of their biometric data in this way but they do not have any way of holding the government accountable as there are no laws in place to regulate this. There is also no regulatory body tasked with the protection of people's privacy or data

[87] Thatcher, Jim, O'Sullivan, David and Mahmoudi, Dillion (n 5).

[88] Al Jazeera (n 3).

[89] Hawkins, Amy (n 60).

protection in Zimbabwe. Zimbabwe's 2002 Access to Information and Protection of Privacy Act does not cover biometric data or cross-border flows of data.[90]

What Does Data Mining Regulation Look Like?

Across the world regulators have been reviewing their data laws. 128 out of the world's 194 countries have passed legislation to secure the protection of data and privacy. In Africa and Asia, 55 per cent of countries have adopted data protection legislation from which 23 are least developed countries.[91] The most widely publicised data law is the European Union's General Data Protection Regulation (GDPR) which set a global benchmark for strengthening individual rights over personal data.[92]

The General Data Protection Regulation

The GDPR came to effect in 2018 being the first major update to European data protection law for over twenty years. Organisations trading in the EU - even if they are registered outside the EU - have to comply with the GDPR, as GDPR obligations apply to organisations located anywhere which process EU citizen's personal data in connection with their offer of goods or services, or their "monitoring'[93] activities.[94] The GDPR gives individuals, known as data subjects much greater control over how organisations process or control the processing of their personal data. The GDPR defines personal data as any information relating to an identified or identifiable natural person[95] including names, identification numbers, location, online identifiers, email address, health records and photos, essentially everything that could identify a living person. Processing is any operation or set of operations that is performed on personal data

[90] Hawkins, Amy (n 60).

[91] UNCTAD, Data Protection and Privacy Legislation Worldwide (2020) https://unctad.org/page/data-protection-and-privacy-legislation-worldwide.

[92] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

[93] Monitoring activities encompass online behavioural marketing activities.

[94] Article 3 Regulation (EU) (n 92).

[95] Article 4(1) Regulation (EU) (n 92).

whether by automated means or not.[96] Data processors are responsible for processing personal data on behalf of data controllers. Data controllers determine the purposes and means of the processing.

Data controllers must therefore demonstrate compliance with six data protection principles under GDPR: First, personal data must be processed lawfully, fairly and in a transparent manner.[97] Secondly, personal data should be collected for specified, explicit and legitimate purposes.[98] Thirdly, personal data should be adequate, relevant and limited to what is necessary.[99] Fourthly, personal data should be accurate and where necessary kept up-to-date.[100] Fifth, personal data should only be retained for as long as is necessary.[101] Finally, personal data should be processed in an appropriate manner to maintain security.[102]

There are also six lawful bases for processing. First, except for special categories of personal data – politics, religion, genetics, sexual orientation, ethnic origin - whose processing is prohibited[103] except upon on certain circumstances, personal data can only be processed if it is necessary to meet contractual obligations entered into by the data subject,[104] to comply with the data controller's legal obligations,[105] to protect the data subject's vital interests,[106] for tasks in the public interest or exercise of authority

[96] Article 4(2) Regulation (EU) (n 92).

[97] Article 5(1)(a)Regulation (EU) (n 92).

[98] Article 5(1)(b)Regulation (EU) (n 92).

[99] Article 5(1)(c) Regulation (EU) (n 92).

[100] Article 5(1)(d) Regulation (EU) (n 92).

[101] Article 5(1)(e) Regulation (EU) (n 92).

[102] Article 5(1)(f) Regulation (EU) (n 92).

[103] Article 9(1) Regulation (EU) (n 92).

[104] Article 6(1)(b) Regulation (EU) (n 92).

[105] Article 6(1)(c) Regulation (EU) (n 92).

[106] Article 6(1)(d) Regulation (EU) (n 92).

vested in the data controller,[107] or for the purpose of legitimate interests pursued by the data controller,[108] or if the data subject gives their explicit consent. Consent can be withdrawn at any time.[110] It has to be as easy to withdraw consent as it was to give it.[111] Consent can be withdrawn via any media. When consent is withdrawn, the organisation will be obliged to erase the individual's data if they are requested to unless an organisation can demonstrate a lawful reason to retain it. In many cases organisations will be able to rely on legitimate interests as the most flexible of the six lawful bases of processing as it could theoretically apply to any kind of processing carried out for any reasonable purpose although the onus will be on organisations to demonstrate their legitimate interests against the personal rights and freedoms of the data subject. Organisations must keep a record of processings[112] which will help with writing privacy notices which must be provided to data subjects directly or indirectly.

As well as the right to be informed,[113] data subjects have other rights which data controllers must be able to facilitate. These are the right of access,[114] the right to rectification,[115] the right to erasure,[116] the right to restrict processing,[117] the right to data portability,[118] the right to object[119] and rights in relation to automated decision-making and profiling.[120]

[107] Artcle 6(1))(e) Regulation (EU) (n 92).

[108] Article 6(1)(f) Regulation (EU) (n 92).

[109] Artcle 6(1)(a) Regulation (EU) (n 92).

[110] Article 7(3) Regulation (EU) (n 92).

[111] Article 7(3) Regulation (EU) (n 92).

[112] Article 30 Regulation (EU) (n 92).

[113] Articles 12-14 Regulation (EU) (n 92).

[114] Article 15 Regulation (EU) (n 92).

[115] Article 16 Regulation (EU) (n 92).

[116] Article 17 Regulation (EU) (n 92).

[117] Article 18 Regulation (EU) (n 92).

[118] Article 20 Regulation (EU) (n 92).

[119] Article 21 Regulation (EU) (n 92).

[120] Article 22 Regulation (EU) (n 92).

Data security is an important part of GDPR compliance. Organisations, and third-party organisations that process data on the behalf of organisations, must implement appropriate and proportionate technical and organisational measures to protect personal data.[121] If an organisation suffers a data breach, reporting it is mandatory under the GPDR. Data processors must report all breaches of personal data to the data controllers and data controllers are required to report breaches to the Information Commissioner's Office within seventy-two hours after discovery if there is a risk to the data subject's rights and freedoms.[122] Data subjects themselves must be notified if there is an undue delay where there is a high risk to their rights and freedoms. If the data is anonymised or encrypted so that it is no longer possible to identify the data subjects there is no risk.[123]

GDPR compliance is not a matter of box-ticking. Demonstrating compliance with the regulation's data protection principles involves taking a risk-based approach to data protection, ensuring appropriate policies and procedures are in place to ensure transparency and accountability on individual's rights. In the GDPR, the principle of accountability is laid out in Article 5(2) which states that a "controller shall be responsible for, and be able to demonstrate compliance with"[124] all six Data Protection Principles of the GDPR as set out in Article 5(1). The burden of proof is imposed on a controller (the entity determining why and how the personal data is processed) to show the organisation is comprehensively compliant.[125] Accountability means having a plan that is documented and implemented and which enables the organisation to prove that it understands what its compliance with the GDPR means.[126] Therefore, building a work-place culture of data privacy and security is also important. Failure to comply

[121] Article 32 Regulation (EU) (n 92).

[122] Article 33 Regulation (EU) (n 92).

[123] See Article 34 Regulation (EU) (n 92).

[124] Article 5(2) Regulation (EU) (n 92).

[125] Brimsted, Kate (2017) 'GDPR series: accountability - a blueprint for GDPR compliance', Privacy & Data Protection, 17(3), 10-12.

[126] Brimsted, Kate (n 125).

with GDPR regulations will leave organisations vulnerable to considerably higher penalties than they have faced under previous data protection legislation, with maximum fines of up to Euros Twenty Million or up to twenty per cent of global turn over whichever is greater.[127]

There are significant advantages to complying with GDPR. GDPR promotes greater transparency and accountability and aims to increase public trust by giving individuals more control over their data. The GDPR does not prevent data-sharing:[128] its aim is to ensure that there is trust and confidence in how organisations use personal data and ensure that data-sharing is fair and secure.[129] By getting data protection right, organisations will improve their reputations and build trust with existing and potential customers. Moreover, by implementing and maintaining the technical and organisational measures required by the GDPR, organisations will benefit from greater levels of information governance and cyber resilience which will help them mitigate the daily onslaught of cyber attacks.

Western regulators through GDPR are able to keep big companies in check by ensuring that they abide by the law. In Africa, laws are weak or non-existent and regulators lack the knowledge and technology to monitor data protection activities. Kenya's Telecoms market regulator, the Communications Authority of Kenya, for example, recently stated that it was not aware of Facebook's installation of any special data mining devices in Facebook's Express Wi-Fi Programme in Kenya.[130] There is a capacity gap that still needs to be addressed in the African context.

[127] See Article 83 Regulation (EU) (n 92).

[128] See Article 1(3)Regulation (EU) (n 92).

[129] Sellars, Claire (2019) 'GDPR: one year on - ICO pulls back the curtain on the impact of the new regime', Computer and Telecommunications Law Review, 25(7), 172-174.

[130] Ochieng' Rapuro (n 74).

Kenya's Legal Framework on Data Protection

Until recently there was no comprehensive regulation on data mining and use of the data of Kenyans by third parties. The Constitution of Kenya 2010, being the supreme law, provides that every person has a right to privacy, which includes the right not to have information relating to their family or private affairs unnecessarily required or revealed;[131] or the privacy of their communications infringed.[132] Although, the Kenya Information and Communications (Consumer Protection) Regulations, 2010 provided for the right to personal privacy and protection against unauthorised use of personal information, they were limited when it came to data mining. The international cross-jurisdictional nature of data mining was in particular a challenge given that most of these apps are provided from outside Kenya's jurisdiction, but are accessible by users in Kenya. Kenya's Data Protection Act 2019 (DPA) was passed to address this issue.

Kenya's DPA was passed following the legal challenge of the Kenya government's *Huduma Namba* digital identity program to fill a lacuna, identified by the courts, of the absence of a comprehensive and effective data protection framework. The DPA borrows heavily from the GDPR. Like the GDPR, the DPA is extraterritorial in nature: it applies as long as the processor or the controller acts upon data of any natural or legal person that is within their jurisdiction.[133] Article 4 GDPR and Section 2 DPA define 'personal data' in the same way, as any information relating to an identified or identifiable natural person. The DPA addresses the relationship between three major parties - data controller; data processor and data subject - whose definitions are similar to those in the GDPR.[134]

[131] Article 31 (c), Constitution of Kenya 2010.

[132] Article 31 (d), Constitution of Kenya (n 131).

[133] Section 4 Data Protection Act No. 24 of 2019.

[134] See Article 4 Regulation (EU) (n 92) and Section 2 Data Protection Act (n 133).

One of the strengths of the DPA is that, like the GDPR it provides for express consent from the data subject.[135] When a breach happens in the handling of data, the individual and the regulating body have to be informed[136] as is the case under GDPR. The DPA also states the safeguards to be considered where a data controller or data processor that uses personal data for commercial purposes as including data encryption and anonymisation through the removal of personal identifying information.[137] The 'right to be forgotten' that is contained in Article 17 GDPR is provided for in s.40(1)(b) DPA which provides that a data subject may request a data controller or data processor to erase or destroy without undue delay personal data that the data controller or data processor is no longer authorised to retain, irrelevant, excessive or obtained unlawfully. The DPA encourages data controllers and processors to appoint a Data Protection Officer to provide advisory on data safety and use as stipulated in the Act.[138] Like the GDPR, the DPA provides for stiff penalties of up-to Kshs. 5 million (approximately USD 50,000).[139]

A major weakness of the DPA is that there is no prescribed time limit on how long an organisation can keep information on a data subject. In addition, there are concerns that the government will use the public authorities exemption to circumvent the overall aim of the DPA through S.30(1)(b)(v) DPA which states that a data controller or data processor shall not process personal data unless the processing is necessary for the performance of any task carried out by a public authority.

Conclusion

At the citizenry level, the ordinary African citizen is hardly aware of data colonialism, let alone being able to push for the appropriate regulation of this issue. Even private actors who are aware and can push for effective regulation of data find themselves in a dilemma because of

[135] Section 37(1)(a) Data Protection Act (n 133).

[136] Section 43(1) Data Protection Act (n 133).

[137] Section 37(2) and Section 41(4)(c)Data Protection Act (n 133).

[138] Section 24 Data Protection Act (n 133).

[139] Section 63 Data Protection Act (n 133).

the narrative that any and all digital development is a net positive. Asking critical questions is almost seen as being an enemy of progress: leaders risk that, by being critical of data colonialism, their people will miss out on the latest advancements in technology and economic development particularly with ready and willing 'development partners' such as the US and China. Africa needs to wake up and realise the potential of its personal data and exercise its information rights with regards to the same.

It remains questionable whether there is an alternative to datified capitalism at this point in time. Under traditional capitalism, labour is a fundamental feature. This is summed up in Adam Smith's labour theory which states that, 'The real price of everything, what everything really costs to the man who wants to acquire it is the toil and trouble of acquiring it.'[140] Unlike the case under capitalism, much of the labour that contributes to data extraction is treated as value-less: as 'just-sharing.'[141] The quasi-labour around digital platforms is often a form of unpaid or underpaid labour and a way in which life is being appropriated for capital.[142] This should not be the case as more transactions are being made into data transactions, that is, transactions configured so as to optimise the extraction of economic value through data. Today's social knowledge is produced through operations that bypass human beings: it is these human beings who are tethered to the discrimination that such knowledge generates through algorithmic reasoning.[143] Strategies for extracting economic profit should stop being presented without dishonesty, that is, as simply proposals to expand knowledge.[144] As Couldry et al put it, 'A continuously trackable life is a disposed life, no matter how one looks at it. Recognizing this dispossession is the start of resistance to data colonialism.'[145]

[140] Wood, John (ed), Adam Smith: Critical Assessments, Volume 3 (Routledge, 1984), 144.

[141] Couldry, Nick and others (n 4).

[142] Couldry, Nick and others (n 4).

[143] Couldry, Nick and others (n 4).

[144] Nick Couldry (n 8).

[145] Couldry, Nick and others (n 4).

Until we get to the stage where we can be honest about our strategies not being afraid about the competition, the key question for law and corporate governance will remain how to safeguard individual, stockholder and corporation data from data mining, whether an organisation can legally and ethically engage in data mining as a growth strategy and whether this is a good thing and the parameters, processes and structures within which it should be legalised. Further research is required now more than ever before on the relationship between information governance, data governance and corporate governance. Boards can no longer bury their heads in the sand and pretend that data mining is not happening. This is a bull that boards will have to take by the horns or be the subject of floodgates of litigation as the public becomes more aware of the existence of data mining. It is also time to ask whether it is necessary to create an international body and court to regulate data mining so that those who engage in ethical data mining do not find themselves disadvantaged to those who do not, and so that those whose rights are violated across jurisdictions can have an avenue where they can air and resolve their grievances. This is the future.

Corporate Governance and Distressed Commercial Banks in Ghana: The Dangers of Excessive Regulation

Dorothy Mamphey & K Wyne Mutuma*[1, 2]

Abstract

This paper seeks to discuss the effects that excessive regulations have had on Ghanian Commercial Banks. The paper will discuss how corporate governance, despite being a solution to corporate failures, can also, if overemphasized upon, stifle the very baby that it has been entrusted to nurse to maturity. Practically, this happened in Ghana between 2016 to 2018 when most banks were either closed or merged with other bigger banks after the regulator adopted robust and radical reforms in the form of legislations or prudential regulations and guidelines that imposed stringent corporate governance principles on commercial banks. This will be discussed in detail by assessing what the regulator got wrong and how it can be resolved. A comparative study will also analyse the prudential guidelines on banks in Kenya and Nigeria and what they got right that eluded the implementation process of the said guidelines in Ghana. Finally, to sum up this paper, there will be recommendations proposed for the identified shortcomings and thereafter a conclusion.

[1] Dorothy Mamphey-Otibo LLB (Walter Sisulu University, Nelson Mandela Bay, South Africa), B.L. (College of Law, University of South Africa) LLL (University of Fort Hare South Africa) Lecturer (General Studies Department, Koforidua Technical University, Ghana); Kenneth Wyne Mutuma Ph.D. (UCT), LLM (UCT), LLB (Liverpool), B-Arch Studies (UON), Senior Lecturer (UON) C.S. and Governance Auditor.

[2] The Bank of Ghana, as part of their policies on banking reforms, issued a directive to give effect, advocate, promote, ensure consistency, and assist in the application of Act 930 to deposit-taking institutions, finance houses, savings and loans, financial holding companies, and banks.