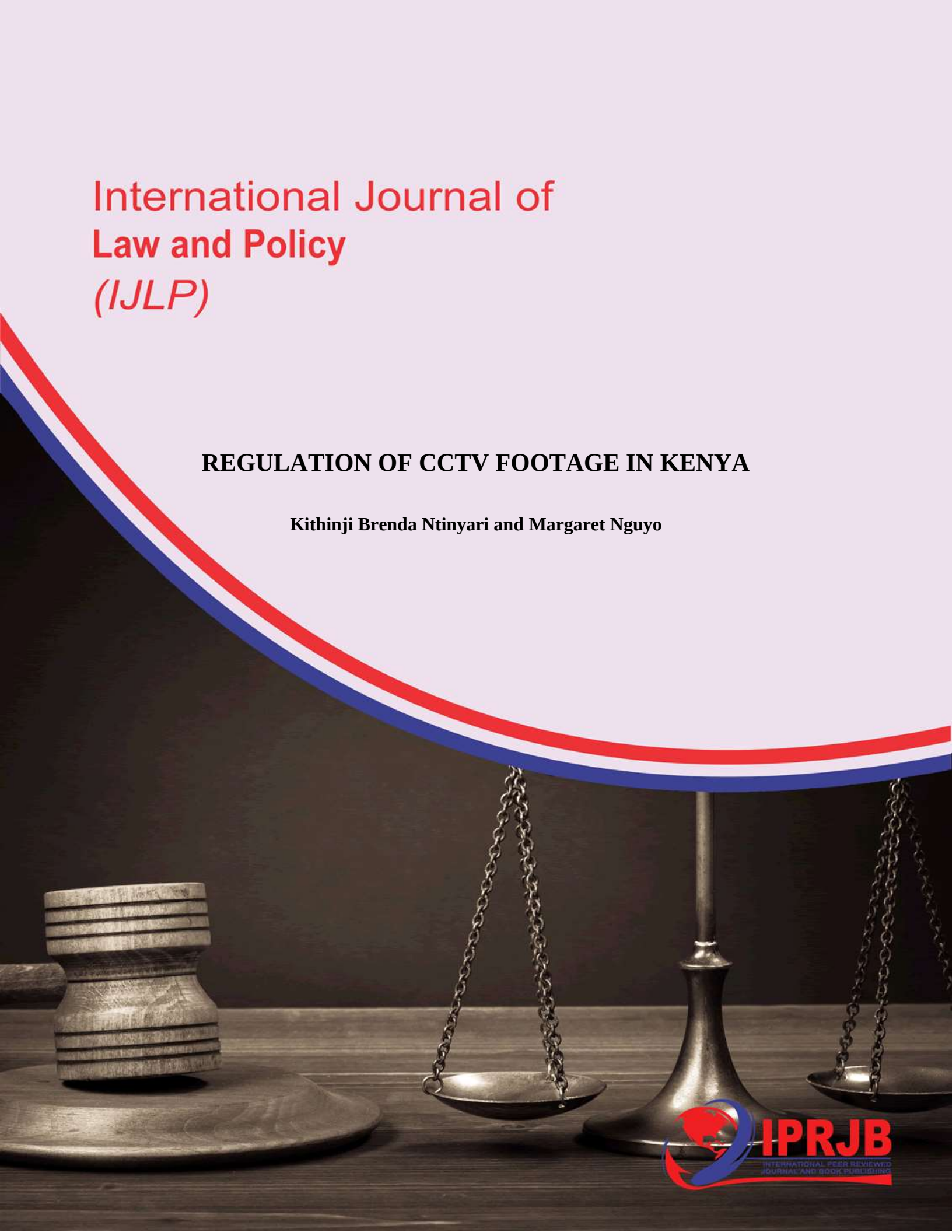
International Journal of
Law and Policy
(IJLP)

REGULATION OF CCTV FOOTAGE IN KENYA

Kithinji Brenda Ntinyari and Margaret Nguyo



International Journal of Law and policy
ISSN xxxx-xxxx (Paper) ISSN XXXX-XXXX (Online)
Vol.1, Issue 2 No.5, pp 58 - 69, 2017

www.iprjb.org

REGULATION OF CCTV FOOTAGE IN KENYA

[1*]Kithinji Brenda Ntinyari

[1]Graduate student, University of Nairobi

Margaret Nguyo

Lecturer, University of Nairobi

[*]Corresponding Email: brendaNtinyari@gmail.com

ABSTRACT

The purpose of this study was to examine the regulations of CCTV footage in Kenya. The methods used in this research include desktop research, having access to online library, statutes, published books and articles. Results showed that regulations of CCTV footage in Kenya is not fully developed. The study recommends the need to ensure that data collected from CCTV is used solely for the purpose meant. This possible by enacting and implementing laws on CCTV installation and use.

Key Words: *regulation, CCTV, footage, Kenya*

In the recent years, there has been an increase in the use of CCTV footages all around the world and Kenya as well has not been left behind. Kenya has experienced an increased installation of CCTV cameras in the major cities like Nairobi and Mombasa and on the major highways. In an effort to curb crime in the major cities, the Kenyan government has installed CCTV cameras on all major highways and in major cities like Mombasa, Kisumu and Nairobi. Despite this effort, there is no legal framework which is in place to regulate the operations of CCTV and how the data collected is used.

By definition CCTV is fully known as Closed Circuit Television is a number of video cameras used to transmit a signal to a particular place on a specific set of monitors.[1] From the definition, the CCTV cameras do capture information of each and every person as they move around public places. As CCTV surveillance becomes more prominent in Kenya, there is need to put in a legal framework to regulate how the footages are being used.

CCTV is a technology which has been in existence for quite a long time as early as the 20th century in the world. Kenya as a developing country has not been left behind in developing this technology. In the 21st century, CCTV is necessary to ensure security as the rate at which crimes are being

[1] www.systems.com/news/all-ininformation-about-cctv-systems.html last accessed on24th June 2016

committed in the towns is increasing each and every day. Closed circuit television are tit is well known as is a television system in which signals are not publicly transmitted but are monitored primarily for surveillance and security purposes.[2] CCTV from its definition is meant to capture images of various individuals and for this reason it is installed in high places and they operate by the use of high quality magnifying cameras which capture clear and accurate video images which can be relied upon for identification purposes.

The crux of this research is to examine the regulation of CCTV footage in Kenya. Kenya does not have specific regulations of CCTV. However there is a Data Protection Bill of 2013 which is yet to be tabled before parliament before it becomes a law. This paper will critically examine whether the proposed Data Protection Bill will effectively regulate CCTV. The UK has a Data Protection Act which regulates the use of CCTV footages. This paper will critically examine how the UK Data Protection Act operates and compare it with the Kenyan Data Protection Bill.

The first CCTV cameras were used back in 1942 by the military in Germany. The military used remote cameras to observe the launch of V2 rockets.[3] In the 1970s and 1980s CCTV were commonly used as an added security measure in the banks. Retail shops also started using CCTV cameras at the same time as a method to both prevent and record any possible crimes which may be carried out.

There was also a need to monitor traffic and Britain was among the first country's to install CCTV for that purpose. They placed them all over their cities to monitor traffic and see if there were any accidents occurring. Since then they have been installed in vehicles and also in private parking lots to prevent any attempts of vandalism.

With the ever advancing technology of CCTV cameras there is need to have them installed in public areas for various reasons. Among the reasons include the fact that CCTV cameras are used to maintain public safety. CCCTV cameras are used to keep an eye out for any crimes that are in progress or even before they start. If a crime is committed in a public area where there was a surveillance camera, the CCTV footage can show a clear image of the criminal making it easier to catch the thief. They can also put up images of the criminal on posters and ask that any member of the public who has any information about the whereabouts of the criminal to report to the nearest relevant authority. The presence of CCTV cameras also serves as a sense of security to the public as no person would want to go into a place where they feel that their security is being threatened. People believe that there are less chances of a crime being committed in a public place where CCTV cameras are installed as the criminals know they are being watched.

The CCTV cameras in public places also prevent crimes. Their installation makes people wanting to commit crimes be cautious as they know they are being captured and can also be used in major cities and stoplights to prevent people from speeding or committing traffic offences. In the 2013 Boston marathon where there were two explosions at the finish line, installation of CCTV cameras is what helped catch the suspects who were linked to the bombing. A CCTV camera which was

[2] http://whatis.techtarget.com/definition/CCTV-closed-circuit-television last accessed 30th July 2016

[3] http://www.covertvideo.com/History_of_CCTV.htm last accessed 3rd September

nearby during the bombing provided a video of the suspects which helped the FBI in tracing the criminals.[4]

The UK has more than 4 million CCTV cameras installed. 75% of the cameras installed in the UK are privately owned while the remaining 25% is government owned. All CCTV controllers are expected to register with the information commissioner's office and ensure that they are operating in accordance with the data protection principles which are provided for under the data protection act.[5]

The UK has a Data Protection Act whose purpose is to ensure that the data collected by CCTV cameras is used solely for the purpose which it was collected for. The purpose therein being referred to is that of helping out in finding out the identity of a person or for monitoring. The data protection directive which regulates the data protection act of 1998 provides that "*member states shall protect the fundamental rights and freedoms of natural persons and in particular their right to privacy with respect to the processing of personal data."*[6]

The purpose of the Data Protection Principles is to protect the interests of the individuals whose personal data is being processed. They apply to everything you do with personal data and include data collected by the CCTV cameras. [7]The first principle of the data protection principles provides that data collected should be processed fairly and lawfully.[8] It further provides that the data collectors should have legitimate grounds for collecting and using individual's personal data in this case especially data collected form CCTV footages. They should also not use the data in ways that have unjustified adverse effects on the individuals concerned or in the CCTV footages. The data controllers should also be transparent about how they intend to use the personal data collected and give the concerned individuals appropriate privacy notices when collecting their data as is required during the installation of CCTV cameras in public places. They should also handle the personal data only in ways that they would reasonably expect and make sure they do not do anything unlawful with the data.

The second principle of data protection provides that any organizations involved in collection of personal data should be open about their purpose for obtaining personal data. The Data Protection Act provides that "*personal data should be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes."* [9]This principle means that organizations should be clear from the outset about what they intend the personal data they are collecting and what they intend to do with the data especially

---

[4] http://www.geekwire.com/2013/security-cameras-helped-catch-boston-marathon-bombers-public-surveillance last accessed 30th august 2016

[5]www.surveillance-and-society.org/articles2(2)/**regulation**.pdf *last accessed 5th September 2016*

[6] Directive95/46/EC,art 1

[7] https://ico.org.uk/for-organisations/guide-to-data-protection/data-protection-principles last accessed 30th September 2016

[8] ibid

[9] UK Data Protection Act 1998

that form CCTV footages in our case. They should also be able to give privacy notices to individuals when collecting their data. After that they should lodge a notice with the office of the information commissioner so as to cover the purpose of use. They should ensure that if they wish to use or disclose the personal data for any purpose that is additional to or different from the originally specified purpose, the new use or disclosure is fair.

Principle three of the Data Protection Act provides that personal data should be adequate, relevant and not excessive in relation to the purpose or purpose for which they are being processed.[10] The data protection principles provide for the adequacy of the data collected. In practice it means that data controllers should hold personal data about an individual that is sufficient for the purpose which they are holding it. For instance the people who are in a CCTV control room should hold only footages that are necessary and delete the unnecessary footages. They should not hold more information than they need for the purpose of security purposes.

The Data Protection Act provides that *"personal data shall be accurate and where necessary kept up to date."*[11] This principle tries to ensure that the data controllers take responsible steps to ensure accuracy of the personal data that they collect. In CCTV instances, data controllers should ensure that the CCTV cameras are located at a place which will capture the necessary data. They should also ensure that their source of data is quite clear so as not to have cases of blurred images. In this sense, CCTV cameras should possess high resolution that can capture clear images that will be accurate and reliable.

The fifth data protection principle provides that data controllers should not retain personal data no longer than is necessary.[12] This practically means data controllers only hold personal data for a short period of time. In cases of CCTV footages, the data collected should possibly be stored for an approximate period of thee moths on a maximum although the Data Protection Act is silent on that. However, they can keep the data for a longer period if it is needed as evidence in a case which is ongoing in court. Data controllers should securely delete any personal data once they are done with it and when the purpose for which they had collected it is done.

The Data Protection Act gives rights to individuals in respect of personal data that organizations hold about them. It provides that *"personal data shall be processed in accordance to the rights of the data subjects under the act."*[13] This principle provides that data subjects have a right to access the copy of information which is being held about them. They also have a right to object to any processing of their personal data if they have reasons to believe that it is likely to cause damage unless in instances when their data is being used as evidence. The data subjects have a right to claim for compensation for damages caused by a breach of their rights under the act.

Principle seven of the data protection principle talks about security. The Data Protection Act provides that *"appropriate technical and organizational measures shall be taken against unlawful*

[10] Supra note 6

[11] Supra 6

[12] Supra 6

[13] Supra 6

processing of personal data and against accidental loss or destruction of or damage to personal property."[14] In practice it means that organizations that have CCTV cameras installed in their premises should have in place appropriate security to prevent the data from being accidentally or deliberately compromised. They will need to have in place specific security measures as to what persons should access the CCTV control room and that there is adequate security. They should also be ready to respond to any breaches of the security swiftly and effectively.

The eighth principle as enshrined in the Data Protection act provides *that "personal data shall not be transferred to a country or territory outside the European economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of their personal data."* In practice data controllers should consider whether it is possible to achieve their objective without sending personal data abroad. They should ensure that they comply with all the other data protection principles before sending personal data abroad. They should also check to ensure that the country or territory where they are sending the personal data provides for adequate protection of the processing of personal data.

The location of the cameras is also an important aspect to ensure that the images captured are in a manner which is specified. In achieving this, the CCTV should only be used to monitor the intended space. Domestic owners also need to be consulted in cases where they border premises which are bring surveyed. The camera systems should be restricted where possible so that they cannot overlook what they are not intended to view. Signs informing the public that they are entering areas covered by CCTV cameras should be clear, visible and legible for all to see. These signs are meant to ensure that the public is informed of the presence of CCTV cameras so that they cannot claim later that their right to privacy was infringed yet they impliedly consented by getting into the areas which are under CCTV surveillance on their own.

In the case of Rynes,[15] Frantisek Ryne installed a surveillance camera after he and he is family were subjected to attacks by unknown people. The CCTV camera filmed a footpath and the entrance to the house opposite his. After someone fired a catapult at his home breaking a window, Rynes gave the CCTV footage recording to the police which helped them in identifying two suspects who were subsequently prosecuted. However, one of the suspects challenged the legality of Ryne's recording. The Czech office found that de it being personal data, he had infringed the data protection rules and was therefore liable for a fine. Ryne's appealed against the ruling as he had only helped identify a criminal. The court ruled in his favor and said that the fact that he had helped catch a criminal absolved him from liability of infringement of data protection rules. It further said that had a crime not been committed then he would be liable as he would have breached data protection principles which are provided for the in Data Protection Act. Court of justice in the European Union further held that where a fixed surveillance camera faced outwards form an individual's private domestic property it captures images of individuals beyond the boundaries of

[14] Supra 6

[15] https://www.theguardian.com/law/2014/dec/11/home-surveillance-cctv-images-may-breach-data-protection-rules-european-court-judgment-says last accessed 18th August 2016

their property, particularly where it monitors the public space, the recording cannot be considered as being for purely a personal or household purpose.[16]

The UK is the most surveilled country in the world with over six million CCTV cameras installed in the country and therefore need arises to look at the challenges it has faced in implementing the Data Protection Act which is the Act used to regulate the use of any personal data collected about the citizens of the country. Article 8 of the European convention on human rights provides that *"everybody has a right to respect for his private and family life, his life and his correspondence."*[17] The issue of privacy is the major challenge that the installations of CCTV cameras has encountered. In the prominent case of **Durant vs. FSA**[18] it was not really an issue of CCTV images but it brought out the real aspect of respect of the right to privacy. In the case, Durant was seeking to have his information which was in the custody of FSA bearing his name or in any way related to him to be shown to him as they had gotten hold of that information as third parties. Individuals claim that they have a right to privacy which is out rightly provided for in the European Convention on Human Rights and also provided for in the UK domestic law in the Human Rights Act. Human right activists who are anti surveillance will advocate for the right to privacy to be protected as opposed to the public duty of security. The fact that the public gets surveyed everywhere in public and as well in private premises brings an issue of transparency. This is so because the public does not know how the information being captured is being used and where it is used. There are several instances where the images captured by CTV cameras are used by fraudsters to defraud innocent members of the public. Therefore one can never be sure as to who has the authority to access the cameras and how they are used especially in private premises and property. There is very little that citizens can do if their private data which has been gathered by CCTV cameras gets in the wrong hands. There is very little that the public can do if their private data which has been captured by CCTV cameras gets in the wrong hands.

As much as private owners will be held accountable for invading into the privacy of others when their security cameras meant to monitor only their property captures other people's property, the issue of accountability comes in as the Data Protection Act only is out to protect public surveillance. Therefore claimants will not have a sufficient law to back their claim when seeking compensation in a court of law. As much as the Data Protection Act places an obligation on the data controllers to have security measures in place to prevent unauthorized access to, alteration, disclosure and or destruction of data there is no specific security measure that a data controller has.

Another challenge is the poor definition of terms in the Data Protection act which makes the interpretation quite difficult for the implementers. Personal data as defined in the act is quite narrow and vague. Personal data defined in the Act is "data which relates to a living individual who can be identified from the data or from those data and other information which is in the possession or is likely to come into the possession of the data controller."[19] From the definition in

[16] https://ico.org.uk/media/1542/cctv-code-of-practice.pdf last accessed 2nd September 2016

[17] European convention on human rights art8(1)

[18] Durant vs. FSA (2003) EWCA Civ 1746`

[19] Uk Data protection act 1998 art 1(1)

the act we can see that it is not quite deep as to personal data as for clarification and the definition of personal data would rather be relating to somebody as opposed to a living individual.

There has also been the issue of the Data Protection Act only being in place to regulate the public use of CCTV cameras and leaving out the domestic users of CCTV out to use them as they so wish. The Data Protection Act has not been able to effectively come up with laws that will regulate domestic users on how to go about CCTV cameras. This thus leaves a great gap as most of the owners of CCTV in the UK are private users and if there is no regulation as to how they should use their CCTV means that some could be malicious and misuse the freedom.

The other problem facing implementation of the Data Protection Act is the lack of a specification as to how long the personal data of citizens can be retained. The Data Protection Act is silent as to how long data controllers should keep the personal data. It just says that data controllers should retain data for as long as it is necessary.

However, the UK has taken measures to deal with the challenges of the Data Protection Act. Some of the measures include the fact that it has come up with a government policy which has been put in place to ensure and provide assurance to individuals that their information will be protected and will be used only for legitimate purposes. The government has also introduced a monetary penalty In the Data Protection Act S.55 A to S.55E to ensure that data controllers who do not take reasonable measures to prevent the most serious breach of the Data Protection principles are liable for a fine as well as an enforcement notice.[20]

In cases where the data is being deliberately and recklessly misused, the government has amended the Data Protection Act to provide an order making power to increase the penalty for such an offense to maximum of a two years imprisonment.[21]

The UK Data Protection Act despite being widely used has proved to have many faults in its application. However, was the UK Data Protection Act implemented in Kenya the same would not be quite effective as Kenya is just a developing country with no major CCTV installations apart from those in major cities and highways to catch traffic and criminal offenders. the Data protection act would serve as a regulator as to who can access the CCTV control room since as at now the CCTV footages has had an issue as to who can access to the camera footages. In some criminal instances where the evidence from the CCTV cameras is expected to be used you will find that there is musing footages and you wonder what happened yet there was a case of unauthorized access to the CCTV control room and the footages which were going to be used are deleted. In the recent probe into the death of the controversial death of business man Jacob Juma, the CCTV cameras show at one point there is a woman in the car which he is driving then minutes later the lady can no longer be seen and there is nowhere on the CCTV cameras that she is seen alighting .this stirs up more questions than answers as no one can tell where the footage went to and the police cannot explain it as well. The UK Data Protection Act was it in force in Kenya would have helped in the control of who can access the data and would impose fines on those found not

[20] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60966/final-report.pdf last accessed 3rd September 2016

[21] Ibid

adhering to the provisions of the Act. However, the issues of privacy would have to be taken into consideration as the constitution in article 31 provides for the right to privacy. Article 31 0f the constitution of Kenya states that every person has a right to privacy, which includes the right not to have;[22]

a) Their person 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 communication infringed.

In light of this then, there is need for the Kenyan government to come up with its own law for the regulation of CCTV cameras. However in Kenya there is a Data Protection Bill of 2013 which is yet to be tabled before parliament for discussion before it becomes a law. The Data Protection Bill is meant to be regulating the collection, retrieval, processing, storage, use and disclosure of personal data which includes data collected by CCTV cameras. By definition personal data as defined in the bill means information about a person including;[23]

a) Information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin or mental health, well being, disability, religion, conscience, belief, culture, language and birth of the individual.
b) Information relating to the education, medical, criminal or employment history of the person or information relating to financial transactions in which the person has been involved in.
c) On identifying number, symbol or other particular assigned to the individual.
d) The fingerprints or blood type of the person.
e) Contact details including telephone numbers of the person.
f) Correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the original correspondence to a third party.
g) A person's view or opinions about another person.
h) Any information given in support or in relation to a grant, award or prize proposed to be made to a person.

The UK Data Protection Act has been of great success to the UK in regulating the data collected from CCTV footages. However it has also encountered many challenges the major one of which we have seen in the research being the issue of privacy. In the light of this foregoing, the same cannot be applied into our system as it is since it has many flaws and the UK as well is on its way to change the Data Protection Act so that it can accommodate the developing technology each and every day. This therefore calls on the Kenyan legislature the department of Information and communications to push for a law to be put in place to regulate the use of CCTV. The Data Protection Bill would be a good starting point for the government and therefore should make efforts to have it brought before parliament so that it can be discussed

[22] Constitution of Kenya 2010

[23] Data protection bill 2013

and become law. The provisions of the Data Protection Bill seem to touch on all the areas that require data protection which includes CCTV and therefore will mark a huge step in the regulation of CCTV footages in the country. The Data Protection Bill however should incorporate clauses that specifically talk about CCTV footages regulation as mere data regulation will not be sufficient enough. The government should however take into consideration the issue of privacy while coming up with the Act so as to ensure that they abide by the provision of the constitution of right to privacy. From the findings of this research, the Kenyan government should take it as a priority to come up with a law that will regulate the use of CCTV cameras as the law should always keep up with new technologies that keep cropping up in the world so as to ensure they do not go unregulated. It should also ensure while making a law to regulate CCTV that they look at both the use of CCTV in both the public and private domestic sector. The UK Data Protection Act puts much focus on the regulation of CCTV footages which are in public but not those used for domestic purposes which should not be the case.

Looking at the Kenya Data Protection Bill it provides for principles that are necessary for data protection. The data protection principles are provided for under article 4 of the bill as follows;[24]

a) Information shall be collected or stored if it is necessary for or directly related to a lawful, explicitly defined purpose and shall not intrude on the privacy of the data subject to an unreasonable extent.
b) Information shall be collected directly form and with the consent of the data subject.
c) The data subject shall be informed of the purpose of any collection of personal information and of the intended recipients of the information at the time of collection.
d) Information shall not be kept for a longer period than is necessary for achieving the purpose for which it was collected.
e) Information should not be distributed in a manner that is incompatible with the purpose for which it was collected with the consent of the person and subject to any notification that would attract objection.
f) Reasonable steps shall be taken to ensure that the information processed is accurate, up-to date and complete.
g) Appropriate technical and organizational measures shall be taken to safeguard the data subjects against the risk of loss, damage, destruction of or unauthorized access to personal information.
h) Data subject have a right to access their personal information and a right to demand correction if such information is inaccurate.

Looking carefully at these data protection principles they are more or less similar to those in use in the UK. This therefore becomes quite tricky knowing Kenya as a country which is poor at implementing its laws and seeing how these laws have not been quite effective in the UK there is need for further research. The information and communication sector experts need to do further

[24] Data Protection Bill 2013

research to come up with a much better law which will regulate the use of CCTV footages as the Data Protection Bill is not as effective.

STATEMENT PROBLEM

Increase in the use of CCTV in Kenya has caused a great need to come up with a regulation of how the footages are to be used. Despite having an Evidence Act which provides guidelines relating to admissibility of such evidence in court, there is still need to have a legal framework which is specific to CCTV footage use. Several jurisdictions around the world have put in place measures seeking to regulate the use of CCTV footages. The UK has a Data Protection Act which seeks to make new provisions for the regulation of the processing of information relating to individuals. The US and Canada also have in place laws regulating how data captured from CCTV footages is used. Kenya as well has a Data Protection Bill which is yet to become law.

Kenya as a developing country also requires an act of parliament to be put in place in order to regulate CCTV footage. Further admissibility of CCTV footage has not been provided for. This study seeks to examine how the UK Data Protection Act has been effective in regulating the CCTV footage and if the same can be applied here in our country. This research aims at evaluating the Kenyan Data Protection Bill with reference to the UK Data Protection Act. The UK Data Protection Act will first be critically analyzed so as to give a basis on its application so as to look at its implementation.

RESEARCH QUESTIONS

How effective is the UK Data Protection Act in regulating CCTV footage?

What challenge has the UK faced in implementing the Act?

Can the Data Protection Act be used here in Kenya?

What the Kenyan Data Protection Bills says about CCTV footages?

Literature review

According to Marianne L.Gras in his article of "The legal regulation of CCTV in Europe" [25]he says that legal regulation of CCTV is simply a body of legal norms to regulate surveillance cameras and their use to observe individuals in a public place. He further says that regulatory bodies in the UK notoriously lack resources and have relied upon the good will and cooperation of those they are regulating and their activities are frequently triggered by a specific complaint.

He goes on to say that the regulation of CCTV in Britain can be at most regarded as potentially for others in terms of good practice. Legal regulation on a micro level is relatively straight forward and has been provided for in many European countries. However, it is more difficult to see how the spirit of constitutional or human rights doctrine can be worked into this scheme, particularly as Data Protection Law may prove to be inappropriate. The efficacy of regulation will depend not

[25] www.surveillance-and-society.org/cctv/html last accessed on 25th June 2016

only on its quality but far more on a country's long term commitment to privacy and the institutional safeguards it has already installed to protect it.

In Peter Wanyonyi's article "In Data Privacy Issues in Citizen Surveillance"[26] he says that provision of security at all levels is perhaps one of the most important functions of any government. In Kenya, a new constitution has developed many governance functions and structures to sub-state counties and security is fast becoming one of the most urgent issues that the counties have to address. He further says that CCTV is a basic technology in practice which is not different from electronic TV except that the images captured by CCTV are not openly transmitted. Apart from capturing and storing images of unwary citizen, it has extensive implications for both privacy and data protection.

Article 31(c) of the Constitution of Kenya protects the right of privacy of Kenyans which includes the right not to have private information unnecessary acquired or revealed.

Recognizable images captured by CCTV cameras are personal data and thus will definitely fall under the Data Protection Act when it becomes law.

The Data Protection Bill of 2012 clause 12 requires that the information so captured should not be kept for longer than is required for purposes for which the information was obtained. In The freedom of Information Bill of 2012, citizens have the right to access information gathered by public entities.

In an article by Lillian Edwards "Switching off the surveillance society? Legal regulation of CCTV in the United Kingdom"[27], she tries to look at whether CCTV footages fall under the category of personal data. The UK Data Protection Act[28] in sec 1(1) defines "personal data" as 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.

Thus CCTV footages capture living individuals which fall under personal data as depicted in the Data Protection Act.

In the case of Durant vs. FSA[29]was not a case concerning CCTV images, but it is recognized to have had a reasonable impact on the regulation of CCTV. In the case, Durant was in dispute with Barclays Bank and made a complaint to the financial Services Authority (FSA) about their behavior which leads to a confidential inquiry into the bank's conduct. Durant, having already filed in various law suits against Barclays, now sought sight of all records held by FSA which mentioned his name or in were in anyway "related" to him. On the grounds that they were personal

[26] https:/www.linkedin.com/pulse20140824044600-14965224-kenya-data-privacy-issues –in-citizen-surveillance last accessed 28th June 2016

[27] Lillian Edwards https:/core.ac.uk/download/files/39/278147.pdf last accessed 30th June 2016

[28] UK Data Protection Act 1998

[29] Durant vs. FSA(2003) EWCA Civ 1746

data of which he was simply the subject and to which by sec 7(1) and sec 8(2) of the Data Protection Act, he thus had right of access.

Lillian Edwards continues to say that in the CCTV context, an equivalent person would ask when an image of an identifiable individual must be obscured or pixelled out before a CCTV tape can be shown to another data subject or to a third party.