Protection of Individuals' Rights to Information in the Digital Environment: An Analysis of Measures in Place

Jane Chebet Malel

Email: *janemalel@yahoo.com; Department of Communication Studies, Moi University, P.O Box 3900-30100, Eldoret, Kenya*

Anne Singoei

Email: **anne.singoei@yahoo.com**;
Department of Communication Studies, Moi University,
P.O Box 3900-30100, Eldoret, Kenya

Abstract

The globalization of economic, political and social activities, supported by an increasing use of information and communication technologies, raises a wide range of questions regarding privacy and the protection of personal data. Countries developing data protection legislation therefore need to be familiar with relevant privacy and data protection issues. We witness an increasing adaptation of "conventional" crime to data protection because of the digitalization, convergence of technologies and globalization of ICT. Traditional measures on investigations do not meet the demands of these changes; therefore special procedures need to be developed. The review sought to investigate the following; mechanisms put in place by the Kenya government and communication stakeholders to aid in data protection, discussed the different types of incidences involving breach of data protection laws and regulations in Kenya, and to give suggestions on ways of improving data protection in Kenya by various communication stakeholders in Kenya. The methodology involves document analysis of relevant documents in the field.

Keywords: *Privacy, Individual Rights, Data protection, Digital environment*

Introduction

The data protection bill kenya,2013,an act of parliament gives effects to Article 31 of the constitution; to regulate the collection, retrieval, processing, storage, use and disclosure of personal data and for connected purpose. Data protection is also referred to as information privacy or data privacy. According to the *Data Protection Act* (1998) of the UK government, the Data Protection Act controls how personal information is used by organizations, businesses or the government.

Everyone who is responsible for using data has to follow strict rules called data protection principles (ibid.). They must make sure that the information is: Used fairly and lawfully, used for limited specifically stated purposes, used in a way that is adequate, relevant and not excessive, accurate, kept for no longer than is absolutely necessary, handled according to people's data protection rights, kept safe and secure, not transferred outside (the country) without adequate protection (the *Data Protection Act* 1998).

An action that breaches any or all or some of the above-stated principles, therefore, amounts to a crime against information privacy. Sensitive information is especially given stronger legal protection by countries. This type of information includes: Ethnic background, Political opinions, Religious beliefs, Health, Sexual health, Criminal records. The globalization of economic, political and social activities, supported by an increasing use of the Internet and other information and communication technologies, raises a wide range of questions regarding privacy and the protection of personal data. This includes questions related to data protection principles, such as those established by the European Union and the Council of Europe (e.g. ETS 108 and Rec R(87)15 on the use of personal data in the police sector), and the investigation of data crime, but also questions related to data retention, the increasing trend towards authentication of ICT users, the relationship between service providers and law enforcement and others.

Objectives

The review was guided by the following research objectives:

i. To identify the types of mechanisms put in place by the Kenya government and communication stakeholders to aid in data protection
ii. To identify different types of incidences involving breach of data protection laws and regulations in Kenya
iii. To make suggestions on ways of improving data protection in Kenya by various communication stakeholders.

Materials and Methods

The methodology involved document analysis of relevant documents in the field of study.

Findings

From the findings; Countries developing data protection legislation need to be familiar with relevant privacy and data protection issues. We see an increasing adaptation of “conventional” crime to data protection because of the digitalization, convergence of technologies and globalization of ICT. Traditional measures on investigations do not meet the demands of these changes; therefore special procedures need to be developed. There is publicly available data from the Internet and other public sources, but also data acquired in the execution of public tasks, often available in governmental databases.

Personal data means any kind of information (a single piece of information or a set of information) that can personally identify an individual or single them out as an individual. The obvious examples are somebody’s name, address, national identification number, date of birth or a photograph. A few perhaps less obvious examples include vehicle registration plate numbers, credit card numbers, fingerprints, IP address (e.g. if used by a person rather than a device, like a web server), or health records. It also has to be noted that personal data is not just information that can be used to identify individuals directly, e.g. by name – it is enough if a person is “singled out” from among other people using a combination of pieces of information or other “identifiers”. For instance, online advertising companies use tracking techniques and assign a person a unique identifier in order to monitor that person’s online behavior, build their “profile” and show offers that could be relevant for this person. Whenever we also browse the internet or send data over networks, we leave electronic traces. These traces can be used to identify us and the people with whom we communicate.

Conclusion

From the review, we can conclude that; data protection has become a key factor in the digital age of communication across the world. As such, Kenya has enacted laws, among other policies and regulations, seeking to protect individuals as well as the media organizations against tendencies towards the abuse of data. Despite all these, there are still cases in which media houses, among other data handlers in Kenya, are reported to abuse data or directly/indirectly allow private and confidential data to get into the wrong hands. These cases raise questions on whether there are regulations, laws and policies that enhance data protection; and if so, to what extent have they been enforced and what are the challenges and opportunities for improving data protection in Kenya?

Bibliography

L.Sweeney,Uniqueness of Simple Demographics in the U.S. Population,LIDAPWP4. Carnegie Mellon University, Laboratory for International Data Privacy,Pittsburgh, PA: 2000. Forthcoming book entitled,The Identifiability of Data.

M. Morgenstern. Security and Inference in multilevel database and knowledge basedsystems.Proc. of the ACM SIGMODConference, pages 357--373, 1987.

Hinke. Inference aggregation detection in database management systems. InProc.of the IEEE Symposium on Research in Security and Privacy, pages 96-107, Oakland,1988.

National Association of Health Data Organizations,A Guide to State-LevelAmbulatory Care Data Collection Activities(Falls Church: National Association ofHealth Data Organizations, Oct. 1996).

Group Insurance Commission testimony before the Massachusetts Health CareCommittee. SeeSession of the Joint Committee on Health Care, Massachusetts StateLegislature, (March 19, 1997).

Cambridge Voters List Database.City of Cambridge, Massachusetts. Cambridge:February 1997.5 Fellegi.On the question of statistical confidentiality.Journal of the AmericanStatistical Association, 1972, pp. 7-18.

J.Kim. A method for limiting disclosure of microdata based on random noise andtransformationProceedings of the Section on Survey Research Methods of theAmerican Statistical Association, 370-374. 1986.

M. Palley and J. Siminoff. Regression methodology based disclosure of a statisticaldatabaseProceedings of the Section on Survey Research Methods of the AmericanStatistical Association382-387. 1986.

G.Duncan and R. Pearson.Enhancing access to data while protectingconfidentiality:prospects for the future. Statistical Science, May, as Invited Paper with Discussion.1991.L. Sweeney.k-anonymity: a model for protecting privacy.International Journal on Uncertainty,Fuzziness and Knowledge-based Systems,10 (5), 2002; 557-570.Page 14.

L.Willenborg and T. De Waal.Statistical Disclosure Control in Practice. SpringerVerlag, 1996.10 T. Su and G. Ozsoyoglu.Controlling FD and MVD inference in multilevel relationaldatabase systems.IEEE Transactions on Knowledge and Data Engineering, 3:474--485, 1991.