International Journal of Scientific Research and Management (IJSRM)
||Volume||11||Issue||03||Pages||EM-2023-4770-4775||2023||
Website: www.ijsrm.in ISSN (e): 2321-3418
DOI: 10.18535/ijsrm/v11i03.em11

Integrity and Confidentiality of Data Protection on Consumers' Privacy in Tanzania: A Case Study of TCRA

Mishael E. Abduel, Kulwa Magingila

Institute of Accountancy Arusha

Abstract
In a world struck by advanced technology in all information and communication parameters, confidentiality and data protection of consumers are vital. However, organisations in diverse business aspects find it challenging to protect consumers' privacy; hence consumers' confidence in business declines. This study focuses on the integrity and confidentiality of data protection on consumers' privacy in Tanzania using TCRA as a case study. The study employed a qualitative approach and a case study design. The researcher preferred purposive sampling, and primary data were collected from 10 respondents who were interviewed. In addition, the study collected qualitative data that were analysed through content analysis. The results of this study revealed that trustworthiness, honesty and responsiveness play a significant role in the integrity and confidentiality of data protection that consequently influences consumers' privacy. Therefore, the study recommends that the government formulate and implement the personal data protection Act. Also, the study recommends reviewing the regulations to include emerging issues in technology like the Internet of Things (IoT), blockchain, big data and social networks.

Keywords: Consent, Data ownership, Data Security, Data Protection Consumers, Privacy Integrity, Confidentiality

1. Introduction

Tanzania's government has established many online services and applications to help users be more connected to government services. These services and applications include an e-Government Electronic Payment Gateway (GePG), an e-immigration system (Passport application), a national ID system and applications, and an electricity payment system (LUKU), to mention a few (Komba-Mlay, 2016). These systems are integrated with banking, mobile, and other private networks and systems; with that, a great amount of data are transferred and stored in these networks and systems. Thus, consumers' privacy can only be achieved and enhanced when these data are protected.

Globally, there have been several practices related to data protection, such as in the USA, European Union, India, China, South Africa and many other countries in the world. In the USA, for example, there are many reported security and data protection breaches facing consumers' electronic devices. These challenges have taken the board BODs to act swiftly on cyber security and protection issues facing users of electronic devices (Al-Sartawi, 2020).

In EU countries, there is a strict practice of data protection through regulations and rules in different sectors, including the health sector, that has created an alarm and a point of discussing issues with the USA. The US would wish for a smooth transfer and sharing of data in areas such as research, treatment, and care, of which tightened rules in the EU restrict the motive (Bradford et al., 2020).

Countries like China and South Korea have greatly advanced in setting up and implementing data security and protection in their countries. Data protection has not only covered cooperate practices but also personal data protection that categorically has supported innovation development in those countries. Therefore, Indonesia has found it indispensable to learn and practice the Chinese and South Korean strategies for enhancing personal data protection through regulations review (Setiawati et al., 2020).

Data protection becomes ineffective if not well guided by legal mechanisms, as the breach cases will be rampant. A case of personal data protection in South Africa where an allegation of misuse of African DNA data in the UK has been observed. This has drawn attention to whether data protection legislation in South Africa is sufficient to serve the purpose (Moodley & Kleinsmidt, 2021).

Enhancing consumer data protection requires a legal framework and an implementation mechanism, such as a board vested with a duty to safeguard the data protection of individuals and organisations, as noted in India. In particular, India has established a council known as the Data Security Council of India (DSCI) with the main duty of protecting the personal data of mobile device users (Bajaj, 2012).

Generally, the integrity and confidentiality of data are becoming a challenge, and consumers need trustworthy, honesty and responsibility from those who manage or store their data (Mambile & Mbogoro, 2020). Such challenges affect the general implementation of the data protection concept even in Tanzania, as highlighted below.

The lack of a comprehensive and appropriate data protection law in place has left many issues not addressed in respect of privacy and data protection (Coleman, 2019). For example, consumer data collected in different applications, systems and networks of organisations are shared with third parties without consumers' consent. In addition, the data ownership issue is a big challenge; for example, when these data are shared on these systems and network organisations, who owns these data? No authority is established to manage, handle and protect these data.

There is also no provision relating to the confidentiality and integrity of data in transit or stored. Neither is it clear if an individual has the right to demand that their personal information be deleted from the records of the parties who collected it, even if this was for legitimate reasons(Elgujja & Arimoro, 2019). Technological practices, if deployed, can help protect data to protect consumers' privacy (Liu et al., 2021). Most of the studies conducted in developing countries, including Tanzania, only examined the importance of e-government in various industries such as; telecommunication services, cybercafé, retailing, restaurants, banking, telecommunication industry, airline catering, local government, hotels, hospitals and education (Davison, 2009).

In this regard, there are limited studies in the context of data protection on consumer privacy in Tanzania. Therefore, this study intends to assess the implementation of data protection on consumers' privacy in Tanzania.

2. Literature Review

For consumers to contribute to the national economy in the industrial revolution era, they need to be confident in the whole business process and the data flow. In this regard, data protection, privacy, and confidentiality are vital. This part reviews studies conducted in different parts of the world on issues related to confidentiality, data protection and the privacy of consumers.

In the context of SNS, the requirement to secure "confidentiality of security of processing" also assumes a new dimension. In order to comply with this criterion, the controller must ensure that the personal data being processed is only revealed to those who "need to know." There are no limitations on who may view the information when the user's profile is set to public. However, even when the profile is set to private, most SNS still do not give users much discretion over which aspects of their profile should be available to which "friends" (Campbell 2021).

Protecting data privacy is still vital to consumers during the pandemic, according to the Cisco Consumer Privacy Survey report titled "Protecting Data Privacy to Maintain Digital Trust." In fact, a third of customers identify as "Privacy Actives," and they have stopped doing business with companies because of their handling of customer data. The survey also revealed that citizens of all 12 countries in the research strongly support current privacy laws and desire greater transparency over how their data is handled (Brill, 2016).

Deloitte also recently published its 2020 Digital Consumer Trends report, primarily concerned with expanding smart device use and data in the UK. It was discovered that customers in the UK are now less worried about how their data is used. For example, 24 percent of respondents in 2019 reported being very concerned, down from 47 percent in 2018. (Edelman et al., 2020).

Consumer data are undoubtedly transforming businesses, and businesses are in charge of managing the data they gather. McKinsey polled 1,000 customers in North America to learn what they thought about consumer privacy and data collecting. We probed them directly about their trust in the companies they use to find out their opinions on data collecting, hacks and breaches, legislation, communications, and specific industries (Lăzăroiu et al., 2020). According to the comments, customers are becoming more deliberate about the kinds of data they share and with whom. They are much more inclined to divulge private information when it is required for them to communicate with an organisation. Consumers feel most at ease exchanging data with healthcare and financial service providers, but no industry has attained a trust rating of 50% for data protection.

This lack of trust is reasonable in light of recent high-profile customer data breaches. Because they were aware of these violations, survey participants' responses about trust were informed. The amount of consumer information exposed in the worst hacks is astonishing. Over 3.5 billion documents were exposed in two breaches at one huge firm. Numerous other companies' breaches made hundreds of millions of records vulnerable. The stakes are high for businesses handling customer data since even those not immediately impacted by the hacks watched how businesses handled them (Hidayat et al., 2021).

Breach of consumer rights in the US has also encouraged the introduction of systems that allow users more control over their data. One in ten internet users globally (and three in ten in the US) use ad-blocking software, which makes it impossible for businesses to trace online behaviour. 87 percent of respondents indicated they would not work with a company if they had reservations about its security procedures. 71 percent of respondents said they would quit business with a company if it disclosed sensitive information without their consent (Pearce & Pinto, 2018).

The way businesses handle customer data, and privacy may become a point of differentiation and potentially a source of competitive business advantage because the stakes are so high, and knowledge of these problems is growing. The main outcomes of our study are summarised here. Then, we provide step-by-step instructions for infrastructure, operations, and data mapping, as well as customer-facing best practices. These can assist businesses in establishing their competitive advantage.

3. Research Methodology

This study was conducted at TCRA in Dar Es Salaam. The organisation was chosen because it is a regulator of all telecommunication issues, including data privacy and the protection of consumers; thus, the organisation has all the necessary data needed for the study. Based on the nature of this study, the qualitative approach seems to be suitable. The approach was complemented by a case study design which allows an in-depth study of a phenomenon. The sample size for the study was 10 employees of TCRA headquarters in Dar Es Salaam. The employees were chosen because they have all the needed information through purposive sampling. A purposive sampling design that was employed in the study is a non-probabilistic sampling design. Data collection involved primary data, which were collected through interviews. In analysing data, the researcher employed the content analysis method, which is among the most reliable methods to analyse qualitative data.

4. Presentation of Findings

This study aimed to assess the integrity and confidentiality of data protection on consumers' privacy in Tanzania by using TCRA as a case study. The study collected primary data through interviews and analysed the data qualitatively through content analysis.

The findings obtained from individual interviews with TCRA staff pointed out that integrity and confidentiality are two principles in CIA Triad that provide a security model that has been developed to help people think about various parts of IT security. Integrity is what the "I" in CIA Triad stands for. Confidentiality is the principle of protecting data from unauthorised access or disclosure. Those with permission to do should only access data or information. Only authorised people can access sensitive information or data. Maintain the privacy and confidentiality of all our secret data. Confidentiality is what the "C" in CIA Triad stands for. These two principles provide a mechanism for ensuring data are protected and give trust to the consumers and make Service Providers responsible for handling and managing consumers' data. Maintaining the consistency, accuracy, correctness and trustworthiness of data and therefore maintaining the privacy of consumers.

The following are the findings based on each sub-variables of assessing integrity and confidentiality of data protection towards consumer privacy.

4.1 Trustworthy

Findings of the data collected from individual interviews at TRCA revealed that trustworthiness is a key component when dealing with consumer privacy. To be effective, organisations need to fully trust the platforms and products they are using. Trust that they work, trust that sensitivity and confidentiality will be protected, and trust that the service providers are giving a high level of partnership and transparency. By doing that, consumers will trust the platforms and ensure their privacy is protected and maintained.

According to **Respondent #10,** during a telephone interview made on the eighth of July 2022, as reported she said,

"…To me, Trustworthy means having a consistent character, even when there is pressure to compromise for data protection. I believe in maintaining the same moral code in all areas of my life, and it is important to me I stay true to my values at all times. People must work hard to show their trustworthiness both in and out of the companies handling and managing data, thus maintaining the privacy of the consumers..."

According to **Respondent # 7,** during a telephone interview made on the ninth of July 2022, the respondent reported that,

'Protecting confidentiality is dependent on being able to define and enforce certain access levels for information. In some cases, doing this involves separating information into various collections that are organised by who needs access to the information and how sensitive that information actually is - i.e. the amount of damage suffered if confidentiality was breached.'

According to **Respondent # 2,** during a telephone interview made on the 14th of July 2022, he said,

'Integrity provides a mechanism of ensuring that unauthorised or undetected changes to data or system configuration do not occur. No modification of data is made. Data stored or data in transit must be correct, and no changes should be made. Maintaining the consistency, accuracy, correctness and trustworthiness of data, some types of attacks may alter records or falsify information.'

Trustworthiness is critical for data protection to make a commitment that builds trust in consumers' privacy. This provides that organisations are reliable, good, honest and effective in protecting consumers' data.

4.2. Honest

Findings of the data collected from individual interviews at TRCA said that honesty is also an important aspect because when a third party get data, they must not disclose or change to an unauthorised part.

According to **Respondent #1,** during a telephone interview made on the eighth of July 2022, he said,

"…I understand that honesty means having characteristics of being trusted and transparent, even when there is pressure to compromise for data protection. If it is dishonest and falsifying for the companies, which manage consumers' information, it may lead to compromising privacy. People must work hard to show their honesties while exchanging data with the third party, thus maintaining the privacy of the consumers..."

Therefore, honesty is crucial to maintain consumer privacy by ensuring that those handling data be honest.

4.3. Responsiveness

Findings of the data collected from individual interviews at TRCA pointed out that responsiveness is part of data protection. It is the commitment to ensuring people handling data are responsible for any breach of data when stored or transmit to third parties. For instance, Respondent #4 reported,

"… Consumers want the organisation to be responsible when protecting their information. Also, accountability for any breach of data must hold people accountable. A great amount of data are collected from various public and government systems and other applications. Therefore, responsibilities of everyone involved must be defined so that whoever breaches data must be accountable...…"

Moreover, **Respondent #6,** during a telephone interview made on 11th of July 2022, reported that,

"…To me, I think people must be accountable for any misuse of customer information. Also, when data re passed to different systems and networks, therefore, there must be a clear role to everyone responsible for consumers' data, if any breach of that data they must be held into account…"

Generally, the findings above based on each sub-variables trustworthiness, honesty and responsiveness of assessing integrity and confidentiality of data protection play a significant role in influencing consumers privacy.

5. Discussion

This study also focused on assessing the integrity and confidentiality of data protection on consumer privacy. Findings from qualitative data that were collected at TCRA through interviews and the existing report indicate that the two variables of integrity and confidentiality of data protection are important.

In addition, sub-variables of trustworthiness, honesty, responsiveness, accuracy, and correctness of data are key issues that must be addressed when assessing the influence of integrity and confidentiality of data protection on consumer privacy. This implies that, despite the regulation for maintaining data protection, there is also a need for integrity and confidentiality for people who handle personal information and favourable measures to enhance consumer privacy.

The aforementioned results are consistent with the Cisco 2020 Consumer Privacy Survey study titled "Protecting Data Privacy to Maintain Digital Trust," which discovered that consumers continue to value data privacy during the epidemic. In fact, a third of customers identify as "Privacy Actives," and they have stopped doing business with companies because of their handling of customer data. The survey also revealed that citizens in all 12 of the participating nations had positive opinions of their privacy laws and demanded greater transparency on the usage of their personal information. Only 28% of respondents said that the epidemic would make privacy less relevant in the future, while 40% felt that it would increase its relevance. Similarly, more than half (57 percent) agreed that businesses should ask about employees' health in order to maintain a safe workplace. However, just 37% of respondents approved of sharing sick person information, 37% approved of location monitoring, and just under 50% approved of sharing information with private companies for research (Weber et al., 2020).

Also recently published was Deloitte's 2020 Digital Consumer Trends Survey, which highlighted the expansion of smart device use and data in the UK. It was discovered that customers in the UK are now less worried about how their data is used. 24 percent of respondents in 2019 reported being very concerned, down from 47 percent in 2018. (Edelman et al. 2020).

Generally, these findings show that to assess the integrity and confidentiality of data protection on consumers' privacy, and one must look at critical issues of trustworthiness, honesty, responsiveness, accuracy, and correctness of data.

Therefore, the findings of this study and the findings of the other studies indicate that consent, data ownership and data protection are the key issues to be addressed in the regulation because they influence much when dealing with consumers' privacy.

6. Conclusion

The comprehensive analysis of this study and the findings of other literature indicates that trustworthiness, honesty and responsiveness are the keys to consumer privacy and data protection. Therefore, assessing the integrity and confidentiality of data protection will contribute to leveraging the industrial revolution

technologies for the national economy by enhancing these two principles of integrity and confidentiality in data so as to maintain security, trust and data protection in the digital economy.

7.0. Recommendation

This study recommends that the Government should Formulate and implement Personal Data Protection Act. Also, it is vital to review the regulations to include the emerging issues in technology like the Internet of Things (IoT), Blockchain, Big data and social networks. Additionally, there is a need for a government to formulate an independent Institution (department, office, organisation, authority) which will deal with handling and managing personal data or information. A good example is Kenya, where they have the so-called Data Protection Authority, the Office of Data Commissioner. The issue of collaboration between the government and private companies should be emphasised to ensure that data are protected and consumer privacy is enhanced.

7. References

1. Al-Sartawi, A. M. A. M. (2020). Information technology governance and cybersecurity at the board level. *International Journal of Critical Infrastructures*, *16*(2). https://doi.org/10.1504/IJCIS.2020.107265
2. Bajaj, K. (2012). Promoting data protection standards through contracts: The case of the data security council of India. *Review of Policy Research*, *29*(1). https://doi.org/10.1111/j.1541-1338.2011.00541.x
3. Bradford, L., Aboy, M., & Liddell, K. (2020). International transfers of health data between the EU and the USA: A sector-specific approach for the USA to ensure an 'adequate' level of protection. In *Journal of Law and the Biosciences* (Vol. 7, Issue 1). https://doi.org/10.1093/jlb/lsaa055
4. Coleman, D. (2019). Digital Colonialism: The 21st Century Scramble for Africa through the Extraction and Control of User Data and the Limitations of Data Protection Laws. *Michigan Journal of Race & Law*, *24.2*. https://doi.org/10.36643/mjrl.24.2.digital
5. Creswell, J. W., & David Creswell, J. (2018). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (5th ed.). SAGE Publications.
6. Elgujja, A., & Arimoro, A. (2019). A review of the patient's right to confidentiality under Saudi Arabian laws. *Preprints*.
7. Komba-Mlay, M. (2016). Adoption of E-Government Services Among Citizens in the Selected Districts of Tanzania. *International Journal of Computer Science And Technology*, *7*(3).
8. Liu, Y., Zhang, J., & Zhan, J. (2021). Privacy protection for fog computing and the internet of things data based on blockchain. *Cluster Computing*, *24*(2). https://doi.org/10.1007/s10586-020-03190-3
9. Mambile, C., & Mbogoro, P. E. (2020). Cybercrime awareness, cyber laws and its practice in public sector Tanzania. In *International Journal of Advanced Technology and Engineering Exploration* (Vol. 7, Issue 68). https://doi.org/10.19101/IJATEE.2020.762051
10. Moodley, K., & Kleinsmidt, A. (2021). Allegations of misuse of African DNA in the UK: Will data protection legislation in South Africa be sufficient to prevent a recurrence? *Developing World Bioethics*, *21*(3). https://doi.org/10.1111/dewb.12277
11. Setiawati, D., Hakim, H. A., & Yoga, F. A. H. (2020). Optimising Personal Data Protection in Indonesia: Lesson Learned from China, South Korea, and Singapore. *Indonesian Comparative Law Review*, *2*(2). https://doi.org/10.18196/iclr.2219