

Data Privacy: Governance of the Hidden Dimension

Dr. Fernando Wangila, Ph.D.,CDP

Abstract:- Data privacy looks at the authorized access of data by defining it in terms of the person who has access to which data, and who does not have access to the same data. Data privacy is wholly dependent on data protection, since one cannot guarantee the privacy of particular data when the same data is not protected by efficient technology. This thus puts data protection as an essential element of data privacy. Data protection laws and regulations are very critical in ensuring data protection because they give guidance on the best practices when it comes to individuals, organizations and the government on how to consume personal data of citizens, thus regulating how personal data is processed. However, governance of such data suffers from a lot of uncertainties, emanating from factors such as technological advancements, inefficiencies in Trans National Data Protection Laws, privacy not being an absolute right, compliance challenges such as lack of ethics, technological convergence and globalization.

I. INTRODUCTION

Data refers to information which has been translated into a form that is effective for processing. This information cuts across all sectors from individual's data, data on government's, data on businesses among other types of data. With an increasingly growing amount of data in the hands of private individuals, organizations, corporations and government, there is need to have proper data management and use. Proper management of data is useful in ensuring important data never leaks to insecure platforms and individuals.

Proper data management calls for the security of data, which is a critical aspect of data management. Protection of data serves to help governments, various companies and individuals from breaches, data theft and losses which can be detrimental to our privacy. Data protection therefore means securing data against access by unauthorized personnel, and this involves the technical measures around the security of data.

Data privacy looks at the authorized access of data by defining it in terms of the person who has access to which data, and who does not have access to the same data. Data privacy is wholly dependent on data protection, since one cannot guarantee the privacy of particular data when the same data is not protected by efficient technology. This thus puts data protection as an essential element of data privacy. If unauthorized individual gains access to personal data of a government, institution or another individual, it puts them under risk since their privacy would no longer be guaranteed. That unauthorized access would therefore put

an individual into the dangers of being charged for theft and other security breaches.

To ensure data privacy, demands that legislations and compliance regulations have to be developed. This is because data privacy is intertwined with the economy, sovereignty and politics as a whole. It is therefore an area that can threaten national security. However, ensuring that all data is protected requires that all legislative and regulatory compliance is adhered to, to the expected that. This may not be always the case and thus makes governance of data privacy incomprehensible. Data privacy remains an extremely contested issue within the modern legal and political discourse. There exist many uncertainties and challenges regarding the governance of data, owing to the amorphous nature of privacy.

II. TECHNOLOGICAL ADVANCEMENTS POSE UNCERTAINTY

Technological advancements are some of the major challenges that put the future of data protection laws at heightened uncertainty levels. Many countries are finding it hard to develop sector-specific data protection laws, especially in sectors such as in the financial sector (Bennett & Raab, 2017). With the advancement of technology, it is obvious that new technologies require new legislative regulations to govern them. This would prove difficult and would therefore mean that protection of data will always be reactionary, lagging behind. Advancements in the field of medicine is equally another major upset in terms of data protection laws, in that advancements in areas such as genetics have proved very difficult to develop sector specific laws, shrouding the whole idea of data privacy laws in uncertainty, meaning comprehensive legislations are difficult to develop.

III. INEFFICIENCIES IN TRANS NATIONAL DATA PROTECTION LAWS

Most individual countries have been able to develop data protection laws to protect their respective citizens over abuses of their private data in the hands of other individuals, organizations or even governments. Directives by international bodies such as the European Nation on member states to adopt data protection legislations, has not received total compliance among all the member countries (Carr, 2015). By establishing particular principles of data protection, such as an individual's right to know where the data originated, the right to rectify inaccurate data and the right of remedy in instances of unlawful processing of data are very essential aspects of legislation on data privacy.

The uncertainty in terms of data protection laws comes when you have citizens from countries with sound data protection laws working in foreign countries that may not have enacted data protection laws, or that the regulations relating to the protection of data vary between the two nations. This will jeopardize the security of data of those individuals.

IV. PRIVACY IS NOT AN ABSOLUTE RIGHT

Most constitutions do not recognize the right to privacy as an absolute right, rather a fundamental right. An absolute right is a legal right that is solely at the discretion of the individual holder. That means the government cannot interfere with that right. A fundamental right is where the government can lawfully interfere with that right under particular circumstances, as laid down in domestic constitutions. This puts legislation geared towards the protection of data at a greater risk from government officials who may impose restrictions that that may be unreasonable to the privacy of their individual data or just choose to act with impunity to punish a particular citizen. Majority of the countries equally make the right to privacy such an amorphous word, that it becomes difficult to appreciate privacy as a right. This jeopardizes the implementation of regulations regarding protection of data, when it is certain that such regulations can be lifted up.

V. COMPLIANCE CHALLENGES, SUCH AS LACK OF ETHICS

Compliance when it comes to the implementation of the laws on data protection may be quite insufficient for our society if those charged with such responsibility do not have the ethical evaluations to steer the implementation in the right place when the legal compliance is already in place. Data protection laws and regulations will lay down what the legal and illegal issues are, but may fail to indicate the best regulations that would ensure efficient data privacy for individuals, corporate and governments among the legal ones. This draws together the position of management when it comes to the implementation of the data protection laws and the place of moral values in governance of data. Analysis of ethical challenges posed by legislation and technological advancements shrouds the very future of data governance.

VI. TECHNOLOGICAL CONVERGENCE

Technological convergence is another aspect of data privacy that puts the governance of data on the spot. This is where technological barriers between systems no longer exist, making the data systems more interoperable with other systems. Legislations on data privacy have had little effect especially because of the sophistication that comes with the technologies ability to process information (Sharma & Alam, 2016). Further developments in medicine, telecommunication and within the transport system and financial systems have caused an upsurge in the information created by every individual. High speed computers with advanced processing systems have been

able to process data on individuals even without a central processing system, leading to overlap of data between various government agencies and even organizations which amounts to breaches in data privacy. This therefore continues to put governance of data in jeopardy.

VII. GLOBALIZATION

Globalization has been able to remove geographical limitations in relation to the flow of data. Various technological developments such as the internet make it difficult to govern the privacy of data. The neutrality in terms of the geographical flow of data makes it available to individuals across the boundaries making restrictions on international data flows challenging. Technological evolution coupled with the increasing value of data makes it difficult to regulate data flows. Laws and regulations regarding the use of media are also often breached despite many pieces of legislation on it. This is easily aided by the ability of individuals to hide their identities, making it extremely difficult to pursue them.

VIII. CONCLUSION

Data protection laws and regulations are very critical because they give guidance on the best practices to individuals, organizations and the governments on how to consume the personal data of citizens, thus regulating how personal data is processed. However, governance of such data suffers from a lot of uncertainties, emanating from factors such as technological advancements, inefficiencies in Trans National Data Protection Laws, privacy not being an absolute right, compliance challenges such as lack of ethics, technological convergence and globalization.

REFERENCES

- [1]. Bennett, C. J., & Raab, C. D. (2017). *The governance of privacy: Policy instruments in global perspective*. Routledge.
- [2]. Carr, M. (2015). Power plays in global internet governance. *Millennium*, 43(2), 640-659.
- [3]. Sharma, I., & Alam, M. A. (2016). Privacy and freedom issues in cyberspace with reference to cyber law. *International Journal of Computer Applications*, 145(3), 11-18.