Data Protection Impact Assessment as a Human Rights Duty of State?

By:

Nelson Otieno Okeyo

November 25, 2022

The Kenyan government has increasingly relied on digital technologies to provide public services. Its recent attempt to roll out a digital ID raised concerns about the misuse of personal data. These concerns eventually led to court action in Ex-parte Katiba Institute & Another. In this case, the High Court stopped the government's decision to roll out the digital ID without a data protection impact assessment (DPIA). The Court then ruled that the duty to conduct DPIA derives from the State obligation to respect the right to privacy, an international human right. This article argues that the finding could mean that the human rights duty of States to respect privacy includes an obligation to conduct DPIA in case of high-risk processing of personal data. This finding appears to have immense potential to cause other African States that do not have data protection laws to conduct DPIA during transitional periods before they adopt data protection laws. The paper further argues that the peculiar circumstances of the case and the litigation approach taken by parties to the

case appears to limit its ability to be an influencing precedent across African jurisdictions and beyond.

Introduction

Though the High Court in Ex-parte Katiba Institute & Another flagged out the retrospective effect of section 31 of the Data Protection Act as an issue for determination its holding in paragraph 15 seems to do more than just answer the question in the affirmative. The Court determined that the obligation to conduct DPIA flows from the State obligation to respect privacy rights, and not necessarily from a data protection law. In this article, I examine the background of the ruling in Ex-parte Katiba Institute & Another. I then examine three factors that, in my view, influenced the court to make its finding. Lastly, I conclude that the ruling has the potential to influence jurisprudence. I further argue that this prospect is dimmed by the prominence of unique aspects of the case that can possibly be fodder for litigants who wish to distinguish the case.

Kenya's Legal Path to Data Protection Law

Between 2010 and 2019

In 2010, Kenyans promulgated the Constitution of Kenya 2010, which repealed the Independence Constitution. The new Constitution provided for express recognition of the right to privacy. It also recognized that international conventions like ICCPR to which Kenya is a party would apply directly to Kenya's domestic legal system pursuant to Article 2(5) of the Constitution.

Since the adoption of the Constitution in 2010, there has been an increase in court cases on alleged breaches of various aspects of privacy and data protection. Parallel to these domestic developments, the United Nations (UN) recognized the need of data protection in the digital age. Though the UN reports and consequential resolutions are not binding, litigants have relied on them as evidence of best practice in Kenyan courts. Buoyed by these local and international, regional privacy and data protection instruments and best practices, Kenya enacted its Data Protection Act in 2019. In December 2021, the Government gazetted three Data Protection Regulations. The Office of the Data Protection Commissioner (ODPC), which oversees the implementation of these frameworks, has also developed a Guidance Note on the conduct of DPIA.

Scope of the Data Protection Act 2019 and the place of DPIA

Data Protection Act 2019 regulates various aspects of data processing. It provides key principles and obligations of data protection as well as the rights of data subjects. It provides for DPIA as a regulatory and compliance approach. Section 31(4) of the Data Protection Act defines DPIA as a process of assessing the impact of envisaged processing operations on the protection of personal data.

The legal framework requires DPIA to be conducted only in instances where a processing operation is likely to result in a high risk to the rights and freedoms of a data subject. According to the Regulations and the ODPC's Guidance Note, the determination of existence of high risk depends on nature, scope, context, and purposes of the data. The process includes iteration of data operations, assessment of their necessity and proportionality, assessment of risks to rights and freedoms and identification of security, safeguard and other measures for mitigating the identified risk.

Implementing the Duty to Conduct DPIA: Ex parte Institute & another

In Kenya, most recent and highly publicized concerns for possible breaches of personal data protection have largely arisen from the operations by the public sectors. Of all the complaints and disputes arising from such cases, the events leading to the court decision in the case of Ex-parte Katiba Institute & Another stand out.

Background to the Ex Parte Institute & another

The decision in Ex-parte Katiba Institute & Another can be traced from 2018 when the Government sponsored an amendment to the Registration of Persons Act cap 107 Laws of Kenya through a Statute Law (Miscellaneous Amendments) Act, 2018 to introduce the digital ID to be known as huduma card. There were suspicions that the Government would collect DNA and GPS coordinates of people as part of implementation of the digital ID. Nubian rights forum and other applicants presented these concerns before the High Court. Eventually, the High Court ruled that the Government could not collect DNA and GPS coordinates as it was intrusive and thus contrary to privacy rights enshrined in Article 31 of the Constitution.

Interestingly, Kenya's data protection legislation was enacted and came into force in November 2019, when the Nubian rights forum case was not yet determined. At the time of the judgment, therefore, the High Court ordered the Government to first operationalize the data protection law including conducting DPIA, before fully implementing digital ID. On 18th November 2020, the Government indicated it would proceed with roll-out without conducting DPIA, a move that prompted Katiba Institute to apply to the court for judicial review in Ex-Parte Katiba Institute & Another.

Court holding

It is useful to note the plan to roll out digital ID was done before 2019. The data protection legislation was passed in 2019 and introduced the requirement to conduct DPIA. The Ex-Parte Katiba Institute & Another was filed after the law was passed.

In finding for the applicants in Ex-Parte Katiba Institute & Another, the judicial review division of the High Court stated that the requirement of DPIA in the 2019 legislation under the Act applied retrospectively, that is before the enactment of the Data Protection Act 2019. Consequently, the court annulled the decision of the Government as contained in its press statement. I am particularly interested in this finding and more especially the rationale and behind paragraph 15 of the ruling that reads:

- '*the duty of State to conduct DPIA does not impose any more obligation or duty on the State than that which the State has in respect to the right to privacy*'

Possible rationale for the decision

The issue before the court was the retroactivity in the application of section 31 of the Data Protection Act. The general rule of statutory interpretation requires Statutes to be presumed as having prospective applications only unless there is a clear parliamentary intention for it to apply retroactively. In any event, a retroactive application must not occasion any injustice or unfairness.

The Government's position in the judicial review cases was that a retroactive application was not warranted. On their part, the applicants submitted that a

retroactive application was possible. So, what influenced the Court to imply the retroactivity and thus arrive at the above-stated finding amidst these competing views?

I have reviewed the judgment and it appears to me that three interrelated factors influenced the decision of the court. I now turn to discuss them below.

Role of State in human rights protection

Under international law, it is the duty of the States to protect, respect and promote human rights. This duty is replicated under the Kenyan Constitution that additionally guarantees protection of the right to privacy. The right to privacy under Article 31 of the Kenyan Constitution is broad. The long title and section 3 of the Data Protection Act provides that the main object of the Statute is to give effect to Article 31 (c) and (d) of the Constitution and ensure the protection of, among others, privacy of individuals.

To the court, at least from paragraphs 96 and 99 of the judgment, the above legislative context formed ‘surrounding circumstances’ enough to imply a clear intention of Parliament to apply the Act retroactively. Therefore, the court seemed to suggest that the retroactivity spans close to 9 years period under which the Constitution had been in operation before the enactment of the Data Protection Act. By adopting this view, the court at paragraph 73 of the judgment endorsed the applicant’s view that the data protection law was a derivative of Article 31 of the Constitution. Additionally, the court considered that the State could not suffer any harm with such an application. Instead, the data subjects would be protected from unfairness arising from collection of personal data.

By taking these views, the court took a human rights approach according to which full and effective implementation of the right to privacy requires adopting safeguard measures to protect the right from all excesses. Consequently, the court adopted an interpretation that shuns the risk of basing an excuse of lack of protection of human rights on lack of legislation as had been the case in the past.

The disobedience attitude of State

The other related factor that appears to have influenced the court decision was the 'attitude of disobedience by the State'. Though there is no express finding based on the impunity of the State, the Court judgment is laced with several expressions of displeasure about how the Government handled the planned roll-out of digital ID. At paragraph 15, the Court referred to what it called 'excesses of State'. Justice Jairus (presiding judge) then proceeds at paragraph 102 to blame the State for not 'acting in good order' in initiating the roll-out without a proper data protection law. The judge also imputes at paragraphs 103 and 104 that by implementing the digital ID in such a manner, the State acted 'unreasonably' and 'put the cart before the horse.

Ideally, all these acts of the State were used to advance the reasoning in the rule of restrictive application of Statutes. For example, the court noted that the State, through its impunity, was the author of its fate. Put simply, the court made the point that retroactivity occasioned no injustice to the State since the latter was the 'author of its own misfortune'.

Yet, the attitude of the State did not just provide the basis for justification for the retroactivity. The judge was particularly worried with the State's insistence to implement digital ID though a court had nullified the law anchoring such an amendment in an earlier case. The judge's frustration is understandable – and made even graver – considering he was part of the three-judge bench that had previously nullified Statute Law (Miscellaneous Amendments) Act, 2018, the law that the Government had used to provide basis for introduction of the digital ID.

Influence of judicial precedent

By the time the court was flagging out the issue of retroactive application of the law, the court in Nubian Rights forum case had held that the provisions of the data protection law applied retroactively to the roll-out of digital ID. Though the ruling stood, no party ever objected that the matter was res judicata. One would expect that the Nubian rights forum ruling was a judgment in rem and bound the court on the issue of retroactivity of the application of the provisions of the Data Protection Act.

All the same, the court flagged the issue at the judgment stage, albeit as an evidential issue. Specifically, the court stated that the import of the judgment was to operate as an estoppel for the government against implementing digital

ID without operationalizing the DPIA framework.

Conclusion

The finding that DPIA does not impose any more obligation or duty on the State than that which the State has in respect to the right to privacy appears to mean that the States activities that involve high risk data processing activities must conduct DPIA, even when they do not have data protection laws. This unique national jurisprudence is likely to influence African jurisprudence to the effect of retroactive application of Data Protection Acts across Africa and beyond. In this case, the court evidently punched above its weight in developing unique arguments to justify its ruling.

However, the above exposition has shown that the jurisprudence seems to have been mainly influenced by specific circumstances of Kenya. That is so considering the unique surrounding circumstances under which it occurred, and which led to the reasoning of court. These unique circumstances may offer fodder for litigants to distinguish the case when litigating similar matters in Kenya and other African jurisdictions.

In the end, I recommend that litigants and advocates should advance similar human rights arguments as advanced by court and suppress possible avenues for distinguishing the case to enhance its jurisprudential application in Kenya, other African States and beyond.

View online: Data Protection Impact Assessment as a Human Rights Duty of State?

Provided by Afronomicslaw