PROPORTIONALITY OF SECURITY LIMITATIONS ON PRIVACY:

A CHECKLIST FOR LEGISLATIVE DRAFTING & INTERPRETATION IN KENYA

CIPIT
CENTRE FOR INTELLECTUAL PROPERTY AND INFORMATION TECHNOLOGY LAW

Strathmore UNIVERSITY

Acknowledgements

We would like to thank Privacy International for making this project possible. We would also like to thank Strathmore University for providing facilitation for the stakeholder workshop. Our sincere thanks goes to: The Supreme Court, Court of Appeal, National Assembly, Senate, The Kenya Law Reform Commission, Law Society of Kenya and Katiba Institute for participating in the workshop.

Table of Contents

I. INTRODUCTION

Innovation in Information Technology (IT) has propelled development, enhanced communication and broadened horizons, while simultaneously complicating our understanding of concepts such as human rights, responsibility over content and security. Worldwide, there is a clamour by states to secure all fronts against security threats which are increasingly involving digital means. It is evident that the need for enhanced and revolutionary security strategies is real and growing. A common method employed by states has been the use of legislation to curb divisive and threatening expression and to grant surveillance powers. However, there have been numerous concerns over the methods employed by different states in achieving security. Many are calling for a balance between enforcing state power and protecting human rights, which are often interfered with in the process.

There exists a number of international standards and domestic constitutional provisions that prescribe the right to privacy; they embody principles that ought to guide any limitations. Despite this, legislative provisions in many countries have been challenged successfully for infringing human rights in a bid to fight insecurity. A succession of quick, reactionary legislative processes can be seen in various jurisdictions. Such an approach is time and resource consuming, and fails to fully address the issue at hand. This shows that there exists a gap in effectively translating existing principles into law when addressing security. The gap can be attributed to the ever-evolving nature of the digital world and the pressing nature of security concerns. There is therefore need to continuously examine how security can be bolstered in a changing world that still upholds democratic values.

There is need for research for guidelines on how to properly mediate the foregoing divide. Such guidelines need to speak to the very essence of legislative drafting by bringing to life the relevant principles of law. These would not only embody laws and international standards, but also enhance foresight at a legislative and interpretive level. Moreover, there is need to equip decision makers with up-to-date knowledge on international standards on privacy and security in the digital world. This project set out to address the stated gap by providing guidelines presented here in the form of a comprehensive checklist. This is a step toward a national framework.

II. BALANCING MECHANISMS FOR COMPETING RIGHTS

Human rights are interdependent and interrelated.[1] However, scenarios often occur within society where different human rights conflict, though they are all protected under law. This is possible as most rights, including privacy, are not absolute. Such scenarios have brought about a need for well thought-out systems, processes and guidelines for reconciling competing rights.[2] Below are different balancing mechanisms and theories as have been developed by different countries, international instruments and scholarly works.

a. The Proportionality principle

This principle aims to determine whether the limitation/interference of a particular right is justifiable.[3] In Kenya, the proportionality principle is embodied in Article 24 of the constitution. Being the supreme law in Kenya, the constitution must be upheld in all legislative, judicial, policy and administrative decisions. Therefore, in seeking a balance of rights, any policy must uphold the standards set out in Article 24 of the Constitution. It also follows that any limitation that is in contravention of this Article is void.

b. A coherent analytical framework for human rights

This theory espoused by Lee, involves a ranking of rights in order of importance as per the context such that some rights take precedence over others.[4]

c. Reconciling rather than balancing rights

Espoused by Lacobucci, who argues that competing rights should be reconciled rather than 'balanced', meaning that the focus ought to be on ensuring the realization of each right as far as possible rather than curbing one in the interest of another.[5]

d. National Policies

Certain jurisdictions have developed policy to enable uniform application of lim-

[1] *United Nations Population Fund, 'Human Rights Principles', 2005.*
[2] *Kofele-Kale N, 'Presumed Guilty: Balancing Competing Rights and Interests in Combating Economic Crimes', The International Lawyer, 40, (2006), 909.*
[3] *Möller K, 'Proportionality: Challenging the critics',*
[4] *Kofele-Kale N, 'Presumed Guilty: Balancing Competing Rights and Interests in Combating Economic Crimes', The International Lawyer, 40, (2006), 909.*
[5] *Szurlej C, 'Reconciling Competing Human Rights in Canada', Peace Research, 47, (2015), 180.*

itation. An example that is often cited is the Ontario Policy on Competing Human Rights.

The Ontario Human Rights Commission has developed a policy guideline on how individuals and institutions may deal with competing human rights. The policy first defines what is meant by 'human rights' and then stipulates key legal principles to be applied. The policy then provides a three-stage test for balancing rights as outlined below.

Stage One: Recognizing competing rights claims

Step 1: What are the claims about?

Step 2: Do claims connect to legitimate rights?

a. Do claims involve individuals or groups rather than operational interests?
b. Do claims connect to human rights, other legal entitlements or bona fide reasonable interests?
c. Do claims fall within the scope of the right when defined in context?

Step 3: Do claims amount to more than minimal interference with rights?

Stage Two: Reconciling competing rights claims

Step 4: Is there a solution that allows enjoyment of each right?

Step 5: If not, is there a "next best" solution?

Stage Three: Making decisions

Decisions must be consistent with human rights and other laws, court decisions, human rights principles and have regard for OHRC policy

At least one claim must fall under the Ontario Human Rights Code to be actionable at the Human Rights Tribunal of Ontario

Three out of four are applicable in Kenya. The analytical framework method may not be applied as Kenyan law does not rank rights and rather, they are regarded as being equal and interdependent. An attempt at reconciling competing rights would therefore be in line with this perspective. The proportionality principle is however embedded into law. Lastly, a national policy is desirable to effect this. Drawing from the foregoing, the following part is a checklist created as a tool in legislative drafting that embodies proportionality and reconciling competing rights.

III. CHECKLIST OF FACTORS TO CONSIDER WHEN LIMITING PRIVACY IN SECURITY PROVISIONS

A provision limiting the right to privacy in deference to national security:

1. Must identify the legitimate corresponding aim pertaining security. (legitimate national security interest)

- A legitimate national security interest should have as its genuine purpose and primary demonstrable effect the protection of national security.[6]
- Where personal data is involved, the legislation must specifically state the persons who are authorised to request access to it, and those authorised to receive such requests.[7]
- Data collected for a specific purpose besides security should not be used for security purposes.[8]
- The burden of proof to demonstrate a legitimate security interest should rest on the government or other agency requesting for acces to personal data.
- Legislations ought to specifically state scenarios that would warrant a limitation of privacy. These aims should not be based on a discriminatory basis, as provided for under Article 27 of the Constitution.

2. Must take into consideration different means of achieving the legitimate security aim identified, and provide for the least restrictive means to be applied.

- Any legislative measures used to safeguard a national security interest should be seen as a means toward this end and should therefore correspond proportionately with the stated national security interest.
- An infringement on any human right, including the right to privacy, should be seen prima facie, as an excessive means unless strictly set out conditions are met. Examples of measures that infringe on digital privacy:
    - *Data retention*

[6]*Definition construed from The Tshwane Principles and The Johannesburg Principles.*
[7]*Worten-Equipamentos Para O Lar Sa v Act (Authority For Working Conditions), Judgment of the Court (Third Chamber) of 30 May 2013.*
[8]*Parliament v Council (Pnr), C-133/06, European Union: Court of Justice of the European Union, 6 May 2008.*

- *Direct access of citizens' communication by a security agency*
- *Back-door access to encrypted information*
- *The mandated removal of encryption altogether*
- *Sharing of data collected with other agencies without the express and informed consent of the subject*
- *Interception of communication, such as mobile/telephone calls, text messages, emails and social media conversations.*
- *Surveillance of persons*

Drafters should ask themselves:

a. Is there already an existing means of achieving the legitimate security interest? If so, the limitation ought not to be legislated as it would not be necessary.
b. If there is no existing means; what are some ways of achieving the stated security interest without limiting privacy?
c. If there are no alternative methods that do not involve a limitation, the limitation on privacy should be accompanied by minimum safeguards on the length of time within which the limitation may be granted, who may have access to the information and that the limitation should be court-sanctioned.

3. Must indicate that the security agency must demonstrate that the measure will not create a security risk for users of authentic systems.

- This is a vulnerability in a computer system that comes about as a result of interference, which makes users prone to security attacks by hackers.
- Guarding against new security risks should be a legally mandated priority for service providers and security agencies involved.
- This will see to the personal and financial security of citizens, as hacking has become a common means of obtaining relevant information. Security efforts should therefore be careful not to leave citizens vulnerable to other looming dangers.

4. Should consider the laws that are already in place that will be affected by the new provision, and to what extent.

- Besides security, privacy is affected by new legislative proposals on various other subject matters such as health, finance, or education.

- The drafters must therefore be aware and take into consideration existing laws to ensure harmony.

5. Must guard against abuse or misuse of systems by members of security agencies and service providers.

- This is to mean that provisions limiting the right to privacy should be mindful of data protection requirements.
- They should be drafted keeping in mind that unfettered access is not unintentionally granted to personnel of security agencies or service providers.
- The necessity for judicial oversight ought to therefore be considered for each limitation on the right to privacy involving security agencies.

6. Should aim to be pre-emptive and futuristic, looking beyond the current situation.

- Drafters ought to take care to look beyond the mischief being addressed at the time, and consider the long-term effects that it will have on the liberties and security efforts in the country.
- Provisions should not be of a nature that curbs the future development of the nation.
- This requires long-sightedness and extensive research on trends in security and privacy to ensure that legislative proposals remain technologically neutral to the best of a drafter's ability.

7. Must be a result of a legislative process that has observed due process, and that involves public participation as much as is practically possible.

- As the digital world is ever evolving, there is need for expert involvement in drafting relevant laws. This will aid in avoiding vague, impractical and outdated provisions.
- Public participation as a constitutional guarantee should be upheld at all times.
- The duration for comment on legislative proposals in this regard, ought to consider the technicality of the audits that are required for privacy impact assessments to be conducted.

8. **Must be reasonable in its effects taking into account all circumstances. The cost of the limitation on privacy should not outweigh the benefit derived to the national security aim.**

- The essential content of the right to privacy should be protected; that is, the dignity and liberty of citizens.
- The drafter ought to consider what the effect of the limitation will mean to the dignity of other citizens, not just the perceived perpetrator.

9. **Must require the security agency and/or involved company to expressly state how the information collected is to be used.**

- The law should require accountability on the part of the state and/service provider before the fact.
- Any economic uses of data collected should be stated, including any partnerships between the state and the service provider.

10. **Must be mindful of data retention principles as security agencies may from time to time need to intercept data in light of ongoing criminal investigation**

- A proportionate criterion ought to be developed to determine the period under which data can be retained by such security agencies.
- Judicial oversight ought to be effected for any further extension to be granted in that regard.

APPENDIX

A. METHODOLOGY

The methodology employed was two-fold: stakeholder engagement and literature review. The stakeholder engagement involved legal researchers and legislative drafters from the Judiciary and Parliament (National Assembly and Senate) respectively; as well as the Kenya Law Reform Commission, Law Society of Kenya and civil society. The goal of this engagement was to get an understanding of the standards and procedures currently used in legislative drafting and interpretation of relevant subject matter and the needs therein. The forum also served as a public participation forum as participants were able to engage with one another and provide insights such as the need for a checklist. The literature review involved a scouring of international instruments and domestic legislation on balancing mechanisms, privacy and security.

B. SCOPE AND DEFINITIONS

a. The right to privacy

Privacy is a protected right under Article 31 of the Constitution of Kenya, and it covers a broad range of areas. Specifically, this right protects an individual from unlawful intrusion and violation of their person in relation to:

- Searches
- Seizure of property
- Information on one's family or private affairs
- Privacy of communications

b. Digital privacy

This is the right to privacy as applied to the internet and other technologies that go beyond the traditional physical spheres such as one's house and physical possessions. Digital privacy has been recognised in Kenyan case law as an aspect of the constitutional right to privacy, and as needing special protection in the technological age.[1] It has been further categorised into three sub-groups:

- Information privacy, also known as **data privacy** refers to the autonomy of a person to dictate who has access to their information.

- Communication privacy refers to the right one has to send and receive communication without interception by a third party.
- The individual's privacy online, free from interference or collection of their data.

A digital right to privacy will be assured where the data subject can determine: a) who can collect their data, b) what data is collected, c) what data is not collected, and d) the nature of consent required to collect certain kinds of data. This criterion derives from the legal doctrine of the right to informational self-determination in respect of right to privacy. It is the right of a person to determine the disclosure, and the use of their personal data.

c. Encryption

This is a process of conversion of plain text or other data into a coded form that can only be accessed by decoding by another person by use of decryption methods such as the use of a key.[9]

d. Data retention

It is the continued storage of an organization's data for compliance or business reasons.[10] It is also known as record retention.

e. Data protection

The process of safeguarding important information from corruption, compromise or loss.[11] These are laws and regulations that make it illegal to store or share some types of information about people without their knowledge or permission.[12]

f. Digital rights

These are the rights of individuals as it pertains to computer access and the ability to use, create and publish digital media.[13]

g. National security

The protection against internal and external threats to Kenya's territorial sovereignty and integrity, its people, their rights, property, peace, stability, prosperity and other national interests.

[9] *Okiya Omtatah Okoiti v Communication Authority of Kenya & 8 others [2018] eKLR Constitutional Petition No. 53 of 2017*
[10] *https://searchsecurity.techtarget.com/definition/encryption accessed on 12 June 2019.*
[11] *https://searchstorage.techtarget.com/definition/data-retention accessed 12th June 2019*
[12] *https://searchdatabackup.techtarget.com/definition/data-protection accessed 12th June 2019*
[13] *https://dictionary.cambridge.org/dictionary/english/data-protection accessed 12th June 2019*
[14] *https://whatis.techtarget.com/definition/digital-rights accessed 12th June 2019*

SOURCES

LEGAL INSTRUMENTS

1. African Union Convention on Cyber Security and Personal Data Protection
2. International Covenant on Civil and Political Rights (ICCPR) 1996
3. General Comment of the United Nations Human Rights Committee on the right of privacy, family, home, correspondence, and protection of honour and reputation (Article 17) of 1988
4. Charter of Fundamental Rights of the European Union
5. United Nations General Assembly Resolution on the right of privacy in the digital age
6. The Santa Clara Principles on Transparency and accountability in Content Moderation
7. 13 International Principles on the Application of Human Rights to Communication Surveillance
8. The Tshwane Principles on National Security and the Right to Information
9. The Johannesburg Principles on National Security, Freedom of Expression and Access to Information, Freedom of Expression and Access to Information, U.N. Doc. E/CN.4/1996/39 (1996).


CIPIT
CENTRE FOR INTELLECTUAL PROPERTY
AND INFORMATION TECHNOLOGY LAW

OUR CONTACTS
CIPIT: Strathmore Law School
3rd Floor, SR. Thomas More Building,
Madaraka Estate, Ole Sangale Road
Nairobi West Area,City Square , Nairobi.
P.O Box 59857 - 00200 Nairobi, Kenya
Tel: (+254) (0)703-034612