PERSONAL DATA PROTECTION IN RELATION TO PRIVACY RIGHTS IN CRIMINAL JUSTICE IN TANZANIA: A CRITICAL APPRAISAL OF ALIGNMENT WITH INTERNATIONAL STANDARDS

Dorah John Mweta[1]

ABSTRACT

The integration of digital technologies in Tanzania's criminal justice system has significantly increased the collection, processing, and storage of personal data, creating both opportunities for efficient law enforcement and challenges for safeguarding privacy rights. This article provides a critical appraisal of **personal data protection in relation to privacy rights** within the Tanzanian criminal justice framework, evaluating the alignment of domestic legal framework with internationally recognized standards. Central to this analysis is the **Data Protection Act**, alongside other relevant statutes such as the Criminal Procedure Act, the **Evidence Act, the Cybercrimes Act, the National Prosecutions Act, the Police Force Act and other relevant laws**, which regulate the handling of personal information during criminal investigations, prosecutions, and law enforcement operations. The study examines the scope, adequacy, and enforcement mechanisms of these legal instruments, focusing on principles such as consent, data minimization, purpose limitation, access, rectification, and institutional accountability. Comparative analysis with international standards, including the **General Data Protection Regulation (GDPR)**, the **United Nations Guidelines for the Regulation of Computerized Personal Data Files**, and regional human rights frameworks, identifies key gaps and inconsistencies. Findings reveal that while Tanzania has made significant strides in codifying privacy protections, challenges persist in operational enforcement, inter-agency coordination, judicial oversight, and public awareness. The study concludes that harmonization with international standards, capacity building for data controllers and the institutionalization of privacy-by-design practices are essential to strengthen the protection of personal data within the criminal justice system, balancing the imperatives of public safety and fundamental privacy rights.

Keywords: Personal Data Protection, Privacy, Criminal Justice, International Standards, Human Rights

[1] LL.B., PGDLP, MPA. Corporate Secretary, VETA.

1. Introduction

The processing of personal data has become an indispensable feature of modern criminal justice systems. Law enforcement agencies increasingly rely on digital databases, biometric identification, electronic surveillance, and cross-border information sharing to investigate and prosecute crime. While these practices may enhance efficiency and security, they simultaneously heighten the risk of unjustified interference with the right to privacy.[1]

In Tanzania, the expansion of data-driven criminal justice practices has coincided with broader legal and policy reforms in the areas of information and communication technology and digital governance. The constitutional protection of privacy under Article 16 of the Constitution of the United Republic of Tanzania, 1977, and the enactment of the Personal Data Protection Act represent significant milestones. However, questions remain as to whether these developments sufficiently regulate the processing of personal data within the criminal justice system in line with international standards.

This article critically examines Tanzania's approach to personal data protection in criminal justice, assessing its alignment with international and regional norms. It adopts a doctrinal and comparative methodology, analyzing legal texts, policy documents, and jurisprudence.

2. Conceptual Framework: Privacy and Personal Data Protection in Criminal Justice

Privacy is widely recognized as a fundamental human right, encompassing both physical and informational dimensions. Informational privacy refers to an individual's ability to control the collection, use, and disclosure of personal information. In criminal justice contexts, this control is necessarily limited; however, international law requires that any limitation be lawful, necessary, and proportionate.

Personal data protection is the legal framework through which informational privacy is operationalized. It consists of principles governing data processing, such as lawfulness, purpose limitation, data minimization, accuracy, storage limitation, security, and

accountability. In criminal justice, these principles must be adapted to the coercive nature of state power and the sensitivity of criminal records, biometric data, and surveillance information.

2.1 Privacy as a Fundamental Right

Privacy has evolved from a common law notion of "the right to be let alone" to a constitutional and human rights guarantee protecting autonomy, dignity, and personal development. It protects individuals from arbitrary interference by public authorities and from unlawful intrusion into personal life.

In international law, privacy is enshrined in the **Universal Declaration of Human Rights (UDHR);[2] the International Covenant on Civil and Political Rights (ICCPR);[3] and the European Convention on Human Rights (ECHR).[4] Indeed, p**rivacy in criminal justice particularly concerns surveillance, search and seizure, communications interception, biometric data collection, DNA databases, and criminal records retention. Thus, privacy is both a **shield against excessive state power** and **procedural safeguard within criminal investigation.**

2.2 Informational Privacy and Data Protection

Modern criminal justice systems rely heavily on digital databases, predictive policing tools, biometric identifiers, and cross-border information exchange. Informational privacy concerns control over personal data, i.e., its collection, processing, storage, and dissemination.[5] Data protection frameworks transform privacy into about seven operational principles which are lawfulness; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality; and accountability.[6]These principles are articulated in Article 5 of the EU General Data Protection Regulation (GDPR).[7] While GDPR primarily addresses civilian data processing, its conceptual

[2] Art. 12.
[3] Art. 17.
[4] Art. 8.
[5] Westin, A.F., *Privacy and Freedom*, New York: Atheneum, 1967, pp. 7–8.
[6] Kuner, C., et al., *The EU General Data Protection Regulation (GDPR): A Commentary,* Oxford: OUP, 2020. Pp. 89–94.
[7] Regulation (EU) 2016/679 (GDPR).

architecture influences criminal justice systems globally, including the EU Law Enforcement Directive.[8]

3. International Standards on Privacy and Data Protection in Criminal Justice

3.1 A General Perspective

The expansion of state surveillance powers and the digitization of criminal justice systems have elevated privacy and personal data protection to central concerns of international human rights law. Criminal investigations increasingly rely on biometric databases, communications interception, cross-border intelligence sharing, and algorithmic data analysis. In this context, international standards seek to balance the legitimate interests of crime prevention and public security with the protection of individual autonomy, dignity, and due process.

3.2 The Legal Foundations

The foundation of international privacy protection lies in two major instruments, which are the **Universal Declaration of Human Rights (UDHR)**[9] and **the International Covenant on Civil and Political Rights (ICCPR)**.[10] Both instruments prohibit arbitrary or unlawful interference with privacy.[11] The Human Rights Committee has clarified that interference must satisfy legality, necessity, and proportionality, and must not be arbitrary even when authorized by law.[12] These principles form the normative baseline for evaluating criminal justice practices worldwide.

At the regional level, **the European Convention on Human Rights (ECHR)**[13] provides a structured proportionality test governing state interference, particularly in surveillance and data retention contexts.[14] The European Court of Human Rights has consistently required adequate safeguards against abuse, especially where secret

[8] Directive 2016/680.
[9] GA Res 217A (III), UN GAOR, 3rd Sess, UN Doc A/810 (10 December 1948).
[10] 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976).
[11] Arts. 12 and 17 respectively.
[12] UN Human Rights Committee, *General Comment No. 16: Article 17 (Right to Privacy)*, UN Doc. HRI/GEN/1/Rev.9 (Vol. I) (1988), paras. 3–4.
[13] European Convention for the Protection of Human Rights and Fundamental Freedoms, 4 November 1950, ETS 5 (entered into force 3 September 1953).
[14] Art. 8(2).

surveillance measures are involved.[15] Similarly, the European Union recognizes data protection as a distinct fundamental right under the EU Charter of Fundamental Rights,[16] further elaborated in the General Data Protection Regulation (GDPR) and Directive (EU) 2016/680 concerning processing of personal data by competent authorities for law enforcement purposes.[17] Beyond Europe, International soft-law instruments such as the **OECD Privacy Guidelines,**[18]and the **UN Guidelines for the Regulation of Computerized Personal Data Files**[19] have shaped global data governance standards, embedding principles such as purpose limitation, data minimization, accuracy, and security safeguards.[20] Although not criminal-justice-specific, these instruments influence national legal systems in structuring lawful data processing by law enforcement authorities.

The African Charter on Human and Peoples' Rights[21] implicitly protects privacy through provisions on human dignity and protection from arbitrary interference.[22] The African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention)[23] provides the most comprehensive regional framework on personal data protection, requiring Member States to regulate law enforcement access to personal data and establish independent supervisory authorities.[24]

3.3 International Jurisprudence, Relevance and Implications for Tanzania

Comparative international jurisprudence provides important interpretative guidance for evaluating Tanzania's protection of personal data within criminal justice processes. Although Tanzania's courts have not yet developed extensive case law on digital privacy, jurisprudence from international and comparative courts, particularly the European Court of Human Rights (ECtHR), the Court of Justice of the European Union

[15]*Klass and Others v. Germany*, App. No. 5029/71, ECtHR (1978), paras. 49–50.
[16] Charter of Fundamental Rights of the European Union [2000] OJ C 326/391 (entered into force 1 December 2009). See Arts. 7 and 8.
[17] Ibid., Arts. 7–8; Regulation (EU) 2016/679 (GDPR), Art. 5; Directive (EU) 2016/680, Arts. 4–8.
[18] (1980, revised 2013).
[19] (1990).
[20] OECD, *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (2013), paras. 7–18; UN General Assembly, *Guidelines for the Regulation of Computerized Personal Data Files*, GA Res. 45/95. (1990), Principles 1–8.
[21] (Adopted 27 June 1981, entered into force 21 October 1986) OAU Doc CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 (1982).
[22]African Charter on Human and Peoples' Rights 1981, arts 4–5, pp 6–7.
[23](Adopted 27 June 2014) AU Doc CAB/LEG/ICT/4(II).
[24]African Union, *Convention on Cyber Security and Personal Data Protection* (2014) arts 8–14, pp 12–18.

(CJEU), South African Constitutional Court, and Kenyan High Court, offers persuasive authority in assessing alignment with international standards such as Article 17 of the International Covenant on Civil and Political Rights (ICCPR).

3.3.1. International Jurisprudence and its Relevance to Tanzania

3.3.1.1 European Court of Human Rights (ECtHR)

In *S and Marper v United Kingdom*,[25] the ECtHR held that indefinite retention of fingerprints and DNA profiles of acquitted persons violated Article 8 of the European Convention on Human Rights, i.e. right to privacy). In this case, the Court emphasized that retention must be necessary and proportionate and that blanket and indiscriminate retention policies are impermissible. The Court further stressed that criminal justice objectives must not override the presumption of innocence or individual dignity.[26] In Tanzania, criminal records and biometric data may be maintained without explicit statutory retention limits.[27] The *Marper* decision suggests that Tanzania should adopt clearer retention and deletion policies, especially for acquitted individuals.

3.3.1.2. Court of Justice of the European Union (CJEU)

In *Digital Rights Ireland Ltd v Minister for Communications,*[28] the CJEU invalidated the EU Data Retention Directive for permitting generalized and indiscriminate retention of communications metadata.[29] In its holding, the court insisted that data retention must be strictly necessary, legislation must provide clear and precise rules governing scope and access, and independent oversight is essential.[30] Similarly, in *Tele2 Sverige AB v Post- och telestyrelsen,*[31] the CJEU reaffirmed that blanket data retention is incompatible with fundamental rights.[32] The relevance of this case to Tanzania pivots on the fact that the Cybercrimes Act authorizes preservation and interception of traffic

[25] (2008) 48 EHRR 50.
[26] Para. 125, p. 116.
[27] See provisions on police records administration under the Police Force and Auxiliary Services Act Cap. 322 R.E. 2002.
[28] Joined Cases C-293/12 and C-594/12 [2014] ECR I-238.
[29] Para. 69, at p. 21.
[30] Paras. 54–68, pp. 18–20.
[31] (Case C-203/15) [2016] ECLI:EU:C:2016:970.
[32] Para. 112, p. 30.

data,[33] but lacks detailed proportionality safeguards comparable to EU standards. These cases underscore the importance of strict necessity, independent oversight, and targeted retention.

3.3.1.3. The South African Constitutional Court

The Court has significantly developed digital privacy jurisprudence. In *AmaBhungane Centre for Investigative Journalism NPC v Minister of Justice*,[34] the Court declared aspects of South Africa's surveillance law unconstitutional for failing to provide adequate safeguards, including post-surveillance notification, independent oversight, and clear data storage limits.[35] The Court emphasized that privacy extends to communications data and metadata in the digital age.[36] Its relevance to Tanzania lays on the fact that albeit Article 16 of the Constitution protects privacy, Tanzanian courts have yet to develop detailed jurisprudence on digital interception. The South African approach demonstrates how constitutional adjudication can strengthen data protection safeguards in criminal justice.

3.3.1.4. Kenyan High Court

The Court has actively reviewed state surveillance measures under Article 31 of the Constitution of Kenya.[37] In *Nubian Rights Forum & Others v Attorney General*,[38] the Court scrutinized biometric data collection under the national identity system, emphasizing that data minimization, legal clarity, proportionality, and safeguards against abuse.[39] Therefore, the Court required robust data protection frameworks before full implementation of biometric systems. This case is relevant to Tanzania in that the Personal Data Protection Act establishes general principles of data minimization and lawful processing,[40] but law enforcement exemptions may weaken their application in criminal investigations. Kenyan jurisprudence demonstrates stronger judicial engagement in enforcing proportionality.

---

[33] Ss. 31–38.
[34] [2021] ZACC 3.
[35] Paras. 134–146.
[36] Paras. 70–78.
[37] 2010 (promulgated on 27 August 2010).
[38] [2020] eKLR.
[39] Paras. 690–720.
[40] Part III.

3.3.2. Implications for Tanzania

The international jurisprudence comparatively reveals four core international principles applicable to criminal justice data protection. These principles are:

3.3.2.1 Strict Necessity and Proportionality, i.e., data collection must be targeted, not blanket.

3.3.2.2 Defined Retention Limits, i.e., indefinite storage of biometric or communication data is impermissible.

3.3.2.2 Independent Oversight, i.e., judicial and regulatory supervision must be meaningful.

3.3.2.4 Effective Remedies, i.e., individuals must have access to redress mechanisms.

Comparative international jurisprudence demonstrates that modern privacy protection in criminal justice requires more than statutory authorization, it demands strict proportionality, independent oversight, and enforceable remedies. While Tanzania has established a foundational framework through the Personal Data Protection Act, and constitutional guarantees, judicial development and legislative refinement are necessary to achieve full alignment with evolving international standards. Drawing from ECtHR, CJEU, South African, and Kenyan jurisprudence would significantly strengthen Tanzania's protection of personal data within criminal justice processes.

4. Tanzania's Legal Framework

4.1 Constitutional Protection of Privacy

The Constitution of the United Republic of Tanzania[41] carries guarantees for respect for personal privacy, family life, and correspondence.[42] It categorically provides that every person is entitled to respect and protection of his person, the privacy of his own person, his family and matrimonial life, and respect and protection of his residence and private communications.[43] This provision establishes privacy as a fundamental constitutional right, forming the basis for legal protection of personal data and private information. However, it allows the State to prescribe legal procedures that determine

[41] Cap 2.
[42] Art. 16.
[43] Ibid.

circumstances, extent, and manner in which the right may be limited without compromising the essence of the right.[44] Therefore, while the provision allows lawful limitations, international standards require that such limitations be clearly prescribed by law and proportionate.

4.2 Statutory Framework on Personal Data Protection

4.2.1. The Data Protection Act.[45]

The Act is the cornerstone of Tanzania's data protection regime. It provides comprehensive rules on the collection, processing, storage, and transfer of personal data across all sectors, including criminal justice. Key provisions relevant to privacy rights include consent and lawful processing, which requires that personal data must be processed lawfully and fairly, and where possible, with the consent of the data subject;[46] data minimization and purpose limitation, which requires that data collected by law enforcement must be adequate, relevant, and limited to what is necessary for criminal investigations;[47] security safeguards, which requires controllers to implement technical and organizational measures to protect personal data from unauthorized access, loss, or alteration;[48] and data subject rights, which emphasizes that individuals have the right to access their data, seek correction, and obtain information on processing activities, which is essential in protecting privacy within criminal justice.[49] In the context of criminal justice, these provisions ensure that investigative and prosecutorial bodies do not arbitrarily infringe upon individual privacy, balancing law enforcement needs with personal data protection.

4.2.2. The Evidence Act.[50]

The Act governs the admissibility of evidence, including electronic and personal data collected during criminal investigations.[51] Sections concerning electronic evidence

[44] Art. 16(2).
[45] Act No. 1 of 2022. Cap 44 R,E 2022.
[46] Ss. 4–6.
[47] S. 5(1).
[48] S. 7(1).
[49] Ss. 8–12.
[50] Cap. 6 R.E. 2022.
[51] Ss. 62–68.

emphasize the integrity, reliability, and lawful collection of data, linking directly to privacy safeguards in criminal investigations.

4.2.3 The Cybercrimes Act.[52]

The Act criminalizes unauthorized access, interception, or misuse of data.[53] It provides both a protective and punitive framework, ensuring that law enforcement actors respect personal data during investigations. The Act complements the Data Protection Act by specifying lawful conditions under which digital evidence may be accessed and used in criminal proceedings. The primary provisions concern unauthorized access to computer systems where it sets out when access is criminal, implying lawful access is required for investigations;[54] interception of communications where conditions for lawful interception by authorities are specified;[55] search, seizure, and preservation of computer data where authority for law enforcement to access digital evidence under controlled and legal conditions are provided;[56] and admissibility of electronic evidence in courts where the legal framework for how digital evidence can be presented and used in criminal proceedings are established.[57]These sections collectively define the **lawful scope for accessing, collecting, preserving, and using digital evidence**, ensuring compliance with privacy and data protection principles outlined in the **Data Protection Act**.

4.2.4. The Penal Code and the Police Force Act.[58]

The Penal Code and the Police Force Act establish criminal investigative powers and law enforcement authority. While these statutes confer powers to collect evidence, they do not provide detailed mechanisms for personal data protection, highlighting the need to integrate principles from the Data Protection Act into policing procedures.

4.3 Criminal Justice Legislation and Practice

[52] Cap 443 R.E. 2023.
[53] Ss. 4–8.
[54] S. 4.
[55] S. 5.
[56] S. 8.
[57] S. 9.
[58] Cap. 16 R.E. 2022 and Cap. 322 R.E 2022 respectively.

4.3.1 A Brief Overview

The protection of personal data within the criminal justice system is intrinsically linked to the right to privacy. In Tanzania, the administration of criminal justice, comprising investigation, arrest, prosecution, adjudication, and correctional services, necessarily involves the collection, processing, storage, and dissemination of personal data. These include biometric data, criminal records, witness statements, and surveillance information. Balancing effective law enforcement with the protection of privacy rights is therefore a constitutional and statutory imperative. This section navigates into the legislative framework governing personal data protection in Tanzania's criminal justice system and evaluates its practical implementation in light of privacy rights.

Just to reiterate, Article 16(1) of the Constitution of the United republic of Tanzania provides that every person is entitled to respect and protection of his person, privacy, and personal security whereas Article 16(2) further prohibits unlawful searches and interference with personal communications. This constitutional guarantee forms the normative foundation upon which criminal justice institutions must regulate the collection and use of personal data. However, Article 30 allows limitation of rights for purposes such as public safety, public order, or national security, provided such limitations are lawful and justifiable. The Personal Data Protection Act regulates the collection, processing, storage, and dissemination of personal data and establishes the Personal Data Protection Commission.[59] It establishes core principles to meet its objectives.[60] In criminal justice practice, these principles are relevant to police investigations; criminal record databases; CCTV and electronic surveillance; and biometric registration systems. However, exemptions exist where processing is necessary for crime prevention, detection, or prosecution.[61]

4.3.2 The Criminal Procedure Act (CPA),[62]

The primary statute governing criminal investigations in Tanzania is the Criminal Procedure Act (which plays a central role in regulating how personal data is collected, accessed, processed, and retained within the criminal justice system. Since criminal

[59] S. 4.
[60] Part III.
[61] See law enforcement exemptions provisions.
[62] Cap. 20 R.E. 2022.

investigations inherently involve the gathering of personal information, such as identity details, biometric data, communications, and digital records, the procedural safeguards governing such collection directly affect the constitutional right to privacy.

4.3.2.1. Search and Seizure under the Criminal Procedure Act (CPA)

(a) Search Warrants and Judicial Authorization

The CPA provides for the issuance of search warrants where the court is satisfied that there are reasonable grounds to believe that evidence relating to an offence may be found in a particular place.[63] This judicial authorization requirement acts as a procedural safeguard against arbitrary intrusion into privacy. The warrant must specify the place to be searched and the items sought, thereby limiting excessive data collection.

(b) Arrest and Personal Search

Upon lawful arrest, police officers are authorized to search the arrested person and seize items connected to the offence.[64] Such searches inevitably involve the collection of personal data such as identification documents, mobile phones, and written communications – to mention but some. While the CPA provides legal authority for such searches, it does not comprehensively regulate the handling, retention, or deletion of the seized personal data hence creating a regulatory gap.

4.3.2.2. Digital Data and Electronic Evidence

Modern criminal investigations frequently involve digital devices and communications data. Albeit the CPA predates contemporary digital realities, courts have interpreted search powers to extend to electronic devices such as mobile phones and computers.[65] Although the CPA provisions do not expressly mention electronic devices, courts have interpreted "things," "property," or "articles" to include **digital devices and electronic data**.[66] This explains therefore that judicial interpretation of search powers under the **Criminal Procedure Act** has gradually expanded to address **electronic devices** such

[63] Ss. 38–45.
[64] Ss. 23 and 50. Also see *Daudi Pete v. Republic* [1993] TLR 22 (CA).
[65] *Director of Public Prosecutions v. Ally Mohamed Ally & Another* (Court of Appeal of Tanzania).
[66] Ibid.

as mobile phones, laptops, and digital storage media, despite the Act originally being drafted with physical premises and tangible property in mind.[67] However, the Act does not expressly define procedures for extraction of digital communications, forensic duplication of data, retention of metadata, and protection of third-party data contained in seized devices. This lack of specificity may risk overbroad data collection, potentially infringing privacy rights.

4.3.2.3. Evaluation: Balancing Criminal Justice and Privacy

The Criminal Procedure Act and related laws in Tanzania establish formal safeguards such as judicial warrants and statutory authorization. However, challenges remain in four issues which are limited regulation of digital searches, broad investigatory powers under cybercrime legislation, absence of detailed retention and deletion rules, and limited transparency and oversight mechanisms. To fully realize privacy rights under Article 16 of the Constitution, criminal procedure must be harmonized with modern data protection standards, ensuring that data collection is necessary, proportionate, and subject to independent oversight.

4.3.3. The Cybercrimes Act: Cybercrime and Electronic Surveillance

The Act empowers law enforcement to investigate cyber offences. It allows interception of communications and preservation of traffic data for investigative purposes.[68] This means the Act supplements criminal procedure by authorizing law enforcement officers to order preservation of traffic data and to intercept communications in certain circumstances.[69] In this case, judicial authorization is generally required for interception; however, the breadth of investigatory powers raises proportionality concerns. The preservation of traffic data, which may include location information and communication metadata, directly implicates informational privacy.[70]

4.3.4. The Police Force and Auxiliary Services Act[71]

In practice, criminal justice agencies collect extensive personal data. Under the Police

[67] *William Ngeleja v. R* (Court of Appeal of Tanzania).
[68] Ss. 31–38.
[69] Ss. 31–38.
[70] S. 32.
[71] Cap. 322 R.E. 2002.

Force and Auxiliary Services Act, the police maintain criminal records and intelligence databases. They collect personal data such as biometric data (such as fingerprints, photographs), criminal history, witness statements, and digital communications. Now, the Act authorizes maintenance of criminal records, yet it provides limited guidance on retention periods or data deletion once an accused is acquitted.[72] This, in turn, raises concerns regarding presumption of innocence, long-term storage of suspect data, and risk of misuse or unauthorized disclosure.

4.4. Practical Challenges in Criminal Justice Data Protection

4.4.1 Data Retention and Storage

There is minimal publicly available regulation concerning retention duration for suspect data, safeguards against unauthorized access, and data breach notification obligations in criminal justice agencies.

4.4.2 Transparency and Accountability

Unlike civilian administrative data processing, criminal investigations often operate under secrecy. While justified for investigative integrity, lack of transparency may hinder effective accountability.

4.4.3 Judicial Oversight

Courts have occasionally emphasized constitutional protections of privacy and fair trial rights. However, jurisprudence specifically addressing data protection in criminal investigations remains limited.

5. International Obligations: Balancing Privacy and Criminal Justice Objectives

Tanzania is party to international human rights instruments recognizing privacy rights, including the International Covenant on Civil and Political Rights,[73] The African Charter on Human and Peoples' Rights, which implicitly protect dignity and integrity.[74]

[72] Ss. 31 - 35.
[73] Art. 17.
[74] Arts. 4–5.

These instruments require that interference with privacy be lawful, necessary, and proportionate.

Following these obligations, the tension between effective crime control and privacy protection is unavoidable. The Tanzanian framework attempts to balance these interests through Constitutional safeguards, statutory authorization for searches and interception, and data protection principles under the Personal Data Protection Act. However, gaps remain in clear digital search standards, independent oversight mechanisms, data retention limits, and remedies for unlawful data processing.

Notwithstanding, Tanzania has made significant progress by enacting the Personal Data Protection Act, which establishes a general legal framework for data protection. Nevertheless, in criminal justice practice, broad law enforcement exemptions, limited oversight, and inadequate regulation of digital investigations pose challenges to the effective realization of privacy rights. Strengthening judicial oversight, clarifying retention policies, and harmonizing criminal procedure laws with data protection principles would enhance compliance with constitutional and international human rights standards.

6. Assessment of Alignment with International Standards

At this juncture, it is unarguable that the regulation of personal data in Tanzania's criminal justice system must be assessed against applicable international human rights and data protection standards. These standards primarily derive from global and regional human rights instruments, as well as emerging international data protection norms. Therefore, this section evaluates the extent to which Tanzania's legal framework aligns with such standards.

6.1. International Legal Framework on Privacy and Data Protection

6.1.1 International Covenant on Civil and Political Rights (ICCPR)

Tanzania is a State Party to the ICCPR,[75] which provides that no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or

[75] United Nations Treaty Collection (UNTC), *International Covenant on Civil and Political Rights*, Status of Treaties, Chapter IV: Human Rights shows that the United Republic of Tanzania acceded on 11 June 1976.

correspondence.[76] The UN Human Rights Committee[77] has clarified that interference with privacy must satisfy three conditions, which are legality, i.e. such interference is provided by law; necessity, and proportionality.[78] In Tanzania, the Constitution protects privacy,[79] while statutory laws

such as the Criminal Procedure Act and Cybercrimes Act provide legal bases for searches and interception. This satisfies the legality requirement. However, concerns arise regarding proportionality, particularly in broad surveillance and data retention practices.

6.1.2 African Charter on Human and Peoples' Rights.

The African Charter does not expressly mention privacy but protects dignity and personal liberty.[80] The African Commission[81] has interpreted these provisions as implicitly protecting privacy interests. Tanzania's criminal procedure framework generally requires judicial authorization for searches and interception, aligning with African human rights principles. However, limited judicial jurisprudence on digital privacy suggests partial rather than full normative development.

6.1.3 International Data Protection Principles

It is a plain fact that Tanzania is not bound by the EU regime that incorporates global data protection standards. These standards are reflected in instruments such as the General Data Protection Regulation (GDPR),[82] which provide persuasive benchmarks. Core principles include lawfulness and fairness, purpose limitation, data minimization, storage limitation, and accountability and oversight.[83] The Personal Data Protection Act

[76] Article 17.
[77] The UN Human Rights Committee (HRC) is a body of independent experts that monitors implementation of the International Covenant on Civil and Political Rights (ICCPR). It was established under Part IV of the ICCPR (Articles 28–45).
[78] Human Rights Committee, General Comment No. 16 (1988), para. 3, at p. 2.
[79] Art. 16.
[80] Arts. 5 and 6 respectively.
[81] The African Commission on Human and Peoples' Rights (ACHPR) is a quasi-judicial body established to promote and protect human rights in Africa. It was created under Article 30 of the African Charter on Human and Peoples' Rights (1981) (commonly called the *Banjul Charter*). The Charter entered into force on 21 October 1986.
[82] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation) [2016] OJ L 119/1.
[83] Arts. 5–6, at pp. 35–36 (Official Journal L119/1).

incorporates many of these principles in Part III. This demonstrates significant legislative alignment with international best practice.

6.1.4. Alignment in Criminal Justice Context

6.1.4.1 Lawfulness of Data Collection

Under the Criminal Procedure Act, searches and seizures require judicial warrants.[84] Similarly, the Cybercrimes Act provides procedures for interception and preservation of data.[85] These statutory frameworks satisfy the international requirement that interference with privacy be provided by law.

6.1.4.2. Necessity and Proportionality

International standards require that data collection be limited to what is necessary for legitimate objectives.[86] While the law provides authorization mechanisms, concerns remain regarding broad investigatory powers in cybercrime enforcement, absence of detailed digital search limitations, and lack of explicit statutory data retention limits in criminal records management. The Police Force and Auxiliary Services Act allows maintenance of criminal records but does not clearly regulate deletion after acquittal.[87]This may conflict with the proportionality principle and presumption of innocence under international human rights law.

6.1.4.3. Oversight and Remedies

It is explicit that international standards emphasize independent oversight and effective remedies for unlawful data processing.[88] The Personal Data Protection Act establishes a Personal Data Protection Commission tasked with oversight.[89] However, the law enforcement exemptions may limit their reach in criminal investigations. Not only that but also judicial remedies for unlawful surveillance remain underdeveloped in practice. Thus, Tanzania demonstrates partial alignment but requires stronger institutional

[84] Ss. 38–45.
[85] Ss. 31–38.
[86] ICCPR, Art. 17; Human Rights Committee, General Comment No. 16, para. 4.
[87] See provisions on police records administration.
[88] Human Rights Committee, General Comment No. 16, para. 10.
[89] Ss. 6–12.

enforcement mechanisms.

Since alignment is partial, the implication is that there are areas of alignment. These areas include constitutional recognition of privacy rights, statutory requirement of warrants for searches, adoption of comprehensive data protection legislation, and establishment of a regulatory authority. These measures reflect compliance with the legality and structural components of international data protection norms. Apart from these areas of alignment, still challenges remain in explicit regulation of digital forensic searches, clear statutory data retention and deletion policies, transparent oversight of intelligence and interception activities, and development of privacy-focused jurisprudence. Without detailed procedural safeguards tailored to digital investigations, the proportionality requirement under Article 17 of the ICCPR may not always be fully satisfied.

To generally say the least, it is in agreement that Tanzania has made significant legislative progress, particularly through the enactment of the Personal Data Protection Act. The framework demonstrates substantial formal alignment with international privacy and data protection standards, especially regarding legality and institutional structure. However, in the criminal justice context, alignment is only partial in terms of proportionality, oversight, and practical enforcement. Strengthening digital safeguards, clarifying retention policies, and enhancing judicial and regulatory oversight would improve Tanzania's conformity with international human rights obligations.

7. Lessons from Selected Jurisdictions

Tanzania's evolving data protection regime reflects growing commitment to informational privacy. However, in the criminal justice context, important lessons may be drawn from comparative jurisdictions such as the European Union (EU), South Africa, and Kenya. These jurisdictions are chosen because they provide useful models for aligning domestic criminal procedure with international standards, particularly Article 17 of the International Covenant on Civil and Political Rights (ICCPR).

7.1. Lessons from the European Union

7.1.1 Strict Necessity and Proportionality Standards

The EU data protection regime, particularly under the General Data Protection Regulation (GDPR), establishes robust principles of lawfulness, data minimization, purpose limitation, and storage limitation.[90] More specifically, criminal justice data processing in the EU is governed by the Law Enforcement Directive,[91] which applies strict safeguards for processing personal data by competent authorities for criminal law purposes.[92] These safeguards include clear legal basis for data processing, independent supervisory authority, defined retention limits, and data subject rights - subject to limited exceptions. Now, while Tanzania's PDPA incorporates general data protection principles,[93] it provides broad exemptions for law enforcement.[94] This being the case, Tanzania could strengthen alignment with international standards by introducing explicit retention limits for criminal records, requiring detailed necessity assessments for digital searches, and enhancing independent oversight over police and intelligence data processing.

7.1.2. Lessons from South Africa

The South Africa's constitutional framework provides a strong model for privacy protection. The Constitution of the Republic of South Africa[95] explicitly guarantees the right to privacy, including protection against unlawful searches and seizure.[96] The Protection of Personal Information Act (POPIA)[97] regulates processing of personal information, including by public bodies.[98] Although certain exemptions apply to national security and law enforcement, these are narrowly construed and subject to oversight by the Information Regulator. The courts in South Africa have also developed strong jurisprudence on proportionality in search and seizure, particularly regarding digital evidence.[99] Therefore, Tanzania has a lesson to learn that constitutional litigation can strengthen privacy jurisprudence in criminal investigations, independent data

[90] Arts. 5–6.
[91] Directive (EU) 2016/680.
[92] Arts. 4–8.
[93] Part III.
[94] Law enforcement exemptions, at p. 27.
[95] 1996 (Act 108 of 1996).
[96] S. 14. Also see *Mistry v Interim National Medical and Dental Council of South Africa* 1998 (4) SA 1127 (CC).
[97] No. 4 of 2013.
[98] Ss. 6–11.
[99] *Minister of Safety and Security v Van der Merwe* 2011 (5) SA 61 (CC); *AmaBhungane Centre for Investigative Journalism NPC v Minister of Justice and Correctional Services* 2021 (3) SA 246 (CC); and *Gaertner and Others v Minister of Finance* 2014 (1) SA 442 (CC).

protection regulators must have meaningful oversight powers over public authorities, and digital search standards should be clearly articulated through legislation or judicial interpretation. Compared to South Africa, Tanzania's constitutional Article 16 provides general protection but has not yet generated extensive digital privacy jurisprudence.

7.1.3. Lessons from Kenya

Kenya offers a regionally relevant model, sharing similar legal traditions with Tanzania.

The Constitution of Kenya expressly guarantees privacy, including protection of communications and personal information.[100] The Kenyan Data Protection Act[101] establishes detailed rules on processing of personal data, registration of data controllers, cross-border data transfers, data subject rights, and oversight by the Office of the Data Protection Commissioner.[102] Kenyan courts have actively reviewed surveillance practices for compliance with constitutional privacy standards.[103] Tanzania has something to learn from Kenya in that explicit constitutional recognition of informational privacy strengthens accountability, judicial enforcement plays a key role in balancing security and privacy, and clear procedural safeguards for interception and surveillance enhance proportionality. Tanzania's Cybercrimes Act authorizes interception and traffic data preservation,[104] but lacks detailed safeguards comparable to Kenya's evolving jurisprudence.

Therefore, Tanzania has made commendable progress through the Personal Data Protection Act. Structurally, the legal framework reflects international standards concerning legality and institutional mechanisms. However, compared to the EU, South Africa, and Kenya, Tanzania's alignment remains substantively partial in the criminal justice sphere. Strengthening proportionality standards, clarifying digital search safeguards, limiting retention periods, and enhancing regulatory oversight would bring Tanzania closer to full compliance with international human rights norms, particularly

[100] Article 31.
[101] No. 24 of 2019 (Laws of Kenya).
[102] Parts III–VI.
[103] *Coalition for Reform and Democracy (CORD) & 2 Others v Republic of Kenya & 10 Others* [2015] eKLR (High Court); *Okiya Omtatah Okoiti & 2 Others v Cabinet Secretary, Ministry of Interior & 3 Others* [2018] eKLR.
[104] Ss. 31–38.

Article 17 of the ICCPR.

8. Conclusion and Recommendations

8.1 Conclusion

Tanzania has made noteworthy legislative and institutional strides in the protection of personal data within the criminal justice system. The enactment of the Personal Data Protection Act (PDPA) provides a formal framework for lawful, fair, and secure processing of personal data. Additionally, constitutional guarantees under Article 16 of the Constitution of the United Republic of Tanzania protect individual privacy, while procedural safeguards in the Criminal Procedure Act, Cybercrimes Act, and Police Force and Auxiliary Services Act establish formal mechanisms for lawful searches, seizure, and data collection. However, a critical appraisal against international standards, particularly Article 17 of the International Covenant on Civil and Political Rights and African human rights instruments, reveals partial alignment. Areas of concern include:

8.1.1 Broad Law Enforcement Exemptions**:** The PDPA allows significant discretion for law enforcement, which may undermine proportionality and necessity principles.

8.1.2 Digital Data Handling Gaps: Current criminal procedure laws do not provide detailed guidance on digital searches, extraction of electronic communications, or secure storage and deletion of data.

8.1.3 Limited Oversight and Remedies: Independent regulatory oversight over law enforcement processing of personal data is weak, and judicial jurisprudence on privacy rights in criminal investigations is underdeveloped.

8.1.4 Retention and Deletion Policies: There is insufficient statutory guidance on retention limits for criminal records, especially in cases of acquittal, risking long-term intrusion into personal privacy.

In comparison, the EU, South Africa, and Kenya provide models with stricter proportionality standards, independent regulatory oversight, clear retention policies, and robust judicial enforcement, offering critical lessons for Tanzania.

8.2. Recommendations

Based on the appraisal made in this article, the following are recommendations on what needs to be done:

8.2.1 To Strengthen Proportionality and Necessity Safeguards

This requires amendment of Criminal Procedure Act to explicitly require necessity and proportionality assessments for all personal data collection, particularly digital evidence. Also, to introduce legal limits on the scope of data that may be seized during investigations.

8.2.2 To Enhance Independent Oversight

This may be done by empowering the Personal Data Protection Commission with authority to supervise and audit law enforcement agencies' compliance with the PDPA. Also, to establish regular reporting requirements on data collection, storage, and retention practices.

8.2.3 To Develop Digital Privacy Protocols

This may be done by enacting regulations specifying standards for forensic digital searches, electronic communications interception, and secure storage of data. Also, to require law enforcement to obtain judicial approval for digital surveillance measures and maintain detailed audit trails.

8.2.4 Introducing Clear Retention and Deletion Policies

This may be done by defining statutory limits for retention of criminal records, biometric data, and electronic evidence. Also, to mandate secure deletion of personal data when an individual is acquitted or charges are dropped.

8.2.5 To Enhance Judicial and Public Awareness

This may be done by promoting judicial training on personal data protection and privacy rights with a view to enhancing case law development. Also, to conduct public awareness campaigns to inform citizens of their rights under the PDPA and the

Constitution.

8.2.6 To Harmonize Domestic Law with International Standards

This may be done by aligning Tanzania's criminal justice data processing practices with ICCPR Article 17 principles, the African Charter, and regional best practices observed in Kenya and South Africa. Also, to integrate lessons from the EU Law Enforcement Directive to ensure data protection principles are consistently applied in criminal justice contexts.

This article considers that by adopting these recommendations, Tanzania can strengthen its alignment with international standards, safeguard citizens' privacy rights, and enhance public trust in the criminal justice system.