OPEN ACCESS

Scholars International Journal of Law, Crime and Justice

Abbreviated Key Title: Sch Int J Law Crime Justice
ISSN 2616-7956 (Print) |ISSN 2617-3484 (Online)
Scholars Middle East Publishers, Dubai, United Arab Emirates
Journal homepage: https://saudijournals.com

Review Article

Biometric Identification System: A Step Towards Better Crime Control in Cameroon

Selvia Lem Tsibong[1*]

[1]Assistant Lecturer, Department of Public Law, Faculty of Law and Political Science, The University of Bamenda, Bambili, North West Region, Cameroon

DOI: https://doi.org/10.36348/sijlcj.2025.v08i06.001 | **Received:** 28.04.2025 | **Accepted:** 04.06.2025 | **Published:** 11.06.2025

***Corresponding author:** Selvia Lem Tsibong
Assistant Lecturer, Department of Public Law, Faculty of Law and Political Science, The University of Bamenda, Bambili, North West Region, Cameroon

Abstract

This study examines biometric identification system as a step towards better crime control in Cameroon, with particular interest to fingerprint biometrics, DNA identification, facial recognition as well as their respective data bases. Cameroon's biometric identification system is a government initiative aimed at enhancing identity management, security, and access to services through the use of biometric technologies. Fingerprint biometrics, DNA identification and facial recognition technologies are used in Cameroon for crime control. Their respective databases are, however, not well developed but for AFIS (Automated Fingerprint Identification System), adopted by Cameroon government as a centralized biometric identification system for managing and authenticating identity documents. International governance on the use of biometrics for crime control has also provided Cameroon with a framework to incorporate the following in its biometric identification system: human right protection, standardization and best practices, accountability, and cross-border crime and cooperation. Legal and institutional frameworks exist that aid in biometric data collection and storage. While biometric identification systems have significant potential for crime control in Cameroon, their current effectiveness is moderate, hampered by infrastructural, legal, and operational challenges. Strengthening legal frameworks, improving infrastructure, ensuring ethical use, and fostering interagency collaboration are essential steps toward maximizing the benefits of biometric technologies in promoting security and justice.

Keywords: Biometrics, Cameroon, Crime Control, Identification System, Legal and Institutional Frameworks.

1. INTRODUCTION

Biometrics-based identification attempts to answer the questions "who are you?" and "are you who you claim to be?" [1]. National identity system has existed for a long time in the history. The very advent of modern forms of citizenship assumes identification [2]. The identification of citizens in Cameroon is tied closely to colonial administration and the post-independence to centralize and modernize governance. During the pre-colonial era, identification was largely informal and based on clan or ethnic group affiliations, local chieftaincies, and oral record-keeping. There were no formal national identity system as social structure and kinship networks served the role of identifying individuals [3]. Cameroon, however, sought to unify its identification system during its post- independence period. The National Identity Card (NIC) was introduced as a formal way to identify citizens. The NIC was paper-based and issued manually, often requiring local authorities' validation [4].

In the wake of the influx global migration, tremendous threat of terrorism, crime and fraud, and the demand for modernization of public services, many

[1] Weicheng S and Tieniu T (1999). Automated Biometrics-Based Personal Identification. Proceedings of the National Academy of Sciences of USA, 96(20): 11065-11066.

[2] Abercrombie, N. *et al* 1986. *Sovereign Individuals of Capitalism*, London: Alen and Unwin; Caplan, J., and Torpey, J. (eds.) 2001. *Documenting Individual Identity*, Princeton NJ: Princeton University Press; Jenkins, R. 2004. *Social Identity*, London: Routledge.
Jones, R. 2000. Digital Rule.

[3] Eugene Arnaud Yombo Sembe. Report on Citizenship Law: Cameroon. RSCAS/GLOBALCIT-CR 2021/13 May 2021.

[4] Ibid.

governments around the world, including Cameroon, are nearly unanimous in their identification policies [5]. The basic function of a national identity system is to link a stream of data with a person [6]. Identification is defined as the act of identifying, the state of being identified or something that identifies one [7]. National identity program is defined as government-initiated program that assigns a unique identification number to each targeted participant, which is used for identification verification [8]. As a matter of fact, when a governmental identification system exists, then an official identity is produced which can then be reproduced in subsequent identification processes. The state makes use of instruments for compulsory registration and identification for each one of its citizens in order to establish such an identity [9].

In addition to this shift towards linking national identity to an electronic registry database, several other changes are also taking place. One is that, at a very intimate level, the means of identification is sought in unique body characteristics. Biometrics is increasingly providing the tools for what is claimed to be accurate identification and verification. National biometric identification systems can significantly aid in crime control by facilitating quicker and more accurate identification of individuals, particularly in the context of law enforcement. Biometrics is used in law enforcement to identify individuals in criminal offenses, prevent wrongful arrest and provide justice to the people. It links individuals to criminal records, identifying potential suspects based on evidence found at crime scenes, and preventing identity fraud. Biometrics is the biological data of individuals representing the identity of each person. The types of biometrics can be divided into two types namely. [10] Biometrics related to physical characteristics, such as fingerprints, hand geometry, voice, retina, facial biometrics, blood type, or DNA and biometrics related to an individual's behavior such as handwriting analysis, cards or information cards.

At present, the situation of crime in Cameroon has a lot going on. Traditional methods of crime control are not enough to control crime. It is imperative for the law enforcement policy to be effective and efficient and with innovations in providing effective services or good policies in order to adequately control crime. A law enforcement development would therefore enhance the efficiency and effectiveness of police operations. This article examines biometric identification system in Cameroon as a step towards better crime control, with particular interest to fingerprint biometrics, DNA identification, facial recognition as well as their respective data bases.

2. Cameroon's Biometric Identification System

Cameroon's biometric identification system is a government initiative aimed at enhancing identity management, security, and access to services through the use of biometric technologies. Several official identification documents such as National Identity Card (NIC), Biometric Passport, Driver's License and Voter's Card, incorporate biometric features such as fingerprinting and facial recognition. In addition, the use of deoxyribonucleic acid (DNA) as a means of identification is an emerging practice that is gradually gaining attention, particularly in criminal investigations, paternity cases, and immigration matters. DNA evidence is increasingly being recognized as a tool to solve crimes, especially in serious cases like homicide and sexual assault. Cameroon has adopted a centralized biometric identification system for managing and authenticating identity documents, often using AFIS (Automated Fingerprint Identification System) and facial recognition software.

2.1. Fingerprint Biometrics

Fingerprint identification has been established as one of the primary means of personal identification. The digitalization of fingerprints and the efficiency offered by automated biometric technology, an attractive prospect for law enforcement and border security agencies around the world, has been widely adopted by governments, including Cameroon, for verifying the identity of suspects in criminal investigations [11]. Fingerprints are suitable for identification purposes due to their uniqueness, constancy throughout life and the fact that the patterns formed are suitable for systematic classification [12]. In addition to the unique nature of fingerprints, their easy accessibility and nonintrusive

[5] Whiety, E. A., & Hosein, G. (2010). Global identity policies and technology: Do we understand the question? *Global Policy*, *1*(2), 209-215.
[6] Clarke, R. (1994). Human identification in information systems: Management challenges and public policy issues. *Information Technology & People*, *7*(4), 6-37.
[7] Ibid.
[8] ITU (2016). *Review of national identity programs*. Geneva: International Telecommunication Union (ITU). Retrieved from https://www.google.com/search?q=where+is+ITU&oq=where+is+ITU&aqs=chrome..69i57j0l5.9868j0j4&sourceid=chrome&ie=UTF-8.
[9] Hornung, G., & Roßnagel, A. (2010). An ID card for the internet—The new German ID card with "electronic proof of identity". *Computer, Law & Security Review*, *26*(2), 151-157.
[10] Kizza, J.M. (2010). Biometrics in: Ethical and social issues in the information age. Texts in Computer Science. Springer, London.
[11] National Science and Technology Council (NTSC). (2006). Privacy and Biometrics: Building a Conceptual Foundation. https://www.hsdl.org/?view&did=463913. Accessed on 19/5/2025.
[12] Jackson, A. & Jackson, J. (2008). Forensic Science (2nd edition), Harlow: Pearson Education; Saferstein,

nature, and their cost effectiveness, have made them the most widely used contemporary form of biometric identification.

In Cameroon, fingerprint evidence is legally recognized and utilized in criminal investigations and judicial proceedings. The Criminal Procedure Code of 2005 provides the framework for the collection and use of such evidence. Specifically, it mandates that upon conviction, an individual's criminal record must include their photograph and fingerprints [13]. Cameroonian law enforcement agencies utilize forensic science, including fingerprint analysis, in criminal investigations. Investigators employ fingerprint kits and photography equipment to collect and analyze evidence from crime scenes [14]. Additionally, Cameroon collaborates with international organizations like Interpol to enhance its biometric capabilities. For instance, under Interpol's Project FIRST, biometric data, including fingerprints, of inmates have been collected and stored in international databases to aid in the identification of individuals involved in transnational crimes [15].

2.1.1. Databases

Automated fingerprint matching databases, developed in the late 1990s and known today as Automated Fingerprint Identification Systems (AFIS), require that an optical device scans and uploads digital images of fingerprints to a centralized database. The distinctive architecture of the fingerprints is analyzed to create a digital template representing key points in the fingerprint. A database operator can search the system to determine the correlation between two or more fingerprints, based on scoring criteria that they nominate. The system automatically produces a list of fingerprints stored in the database that have the closest match. Following this, a human fingerprint expert with many years of training in the field makes the final determination on whether the fingerprints match and belong to the same individual [16]

Automated databases used by law enforcement are typically comprised of two subsystems: a ten-print criminal identification system comprising a set of fingerprints obtained through an arrest or during the course of an investigation; and prints that are on file comprising latent fingerprints that have been obtained from crime scenes or physical evidence [17]. These subsystems enable fingerprint databases to conduct the following four types of searches: print-to-print searches: these are conducted to verify the identity of a suspect through a comparison of fingerprints obtained from a suspect against fingerprints stored in the database; mark-to-print searches: these are conducted in order to compare a fingerprint obtained from a crime scene, or other physical evidence, against fingerprints held within the database; print-to-mark searches: these are used to determine whether an individual is linked to other crime scenes by comparing their fingerprints against all the fingerprints held within the database, but in instances where previous searches have failed to produce a match; mark-to-mark searches: used to determine if a fingerprint obtained from a crime scene or physical evidence is connected with other prints held within the database [18].

AFIS have now been established in many jurisdictions around the world and Cameroon has developed a comprehensive biometric identification system that includes the collection of ten fingerprints and facial data from citizens. This data is stored in the AFIS, which supports the issuance of biometric national ID cards. As of the latest updates, over 20 million records have been enrolled, incorporating both new and legacy data [19]. The biometric ID cards feature embedded chips containing personal and biometric information, including fingerprints. These cards are designed to enhance identity verification processes and reduce identity fraud [20]. Fingerprint scans are used for biometric enrollment in visa applications and are also part of national ID systems [21].

2.2. DNA Identification

DNA identification is the most significant scientific advancement in the history of forensic science as it plays an important role in modern criminal investigations of serious crimes. DNA can be recovered from most biological material. The most common human biological materials submitted for testing are blood,

R. (2015). Criminalistics: An Introduction to Forensic Science. Harlow: Pearson Education.

[13] Section 577 of the 2005 Cameroon Criminal Procedure Code (CCPC).

[14] Tsibong, S. L. (2023). The use of forensic science in the criminal justice system of Cameroon. PhD Thesis within the framework of the doctorate program in Criminology at Selinus University of Sciences and Literature, Italy.

[15] Biometric Updates (2024). Interpol program for fighting terrorism through biometrics deployed in Cameroon. https://www.biometricupdate.com. Accessed on 18/5/2025.

[16] Milne, R. (2013). Forensic Intelligence. Boca Raton, FL: CRC Press.

[17] Moses *et al.,* (2010).

[18] Ibid.

[19] Cameroon Delivers on Digital ID-CybAfriqué Newsletter, March 8, 2025. https://cybafrique.substack.com/p/cameroon-delivers-on-digital-id?utm_source=chatgpt.com. Accessed on 18/5/2025.

[20]Cameroon Launches Advanced Biometric National ID System with 48-Hour Issuance Promise- IDtech Wire, February 24, 2025. https://idtechwire.com. Accessed on 18/5/2025.

[21] VFS GLOBAL. What happens at the Visa Application Centre. https://visa.vfsglobal.com/cmr/en/can/attend-centre/what-happens-at-centre. Accessed on 19/4/2025.

semen, hair, saliva, skin and sweat. It can be obtained by analysing material present on personal items such as razors, hairbrushes or toothbrushes. DNA evidence is used to link or exclude an individual from association with the crime scene. The sample collection must accord with standard procedure, and a chain of custody must be established to enable DNA evidence to be used at trial [22].

The comparison of DNA profiles obtained from a crime scene with those from a suspect or database, is widely used in cases involving serious crimes against the person, particularly homicide and sexual assault. A range of new techniques of DNA identification continue to be developed and applied in criminal investigations around the world [23].

In Cameroon, the Criminal Procedure Code [24], outlines procedures for criminal investigations and evidence handling. However, it lacks specific guidelines on the collection, analysis, and admissibility of DNA evidence. This absence of detailed legislation means that the use of DNA in criminal cases operates without a standardized legal framework, potentially impacting its effectiveness and reliability in judicial proceedings. Initiatives are, however, underway to develop a comprehensive legal framework for DNA evidence in Cameroon. For instance, the Forensic DNA Policy Board for Africa aims to draft standardized policies and legislation to guide the use of DNA in criminal justice systems across the continent, including Cameroon. These efforts focus on establishing clear protocols for DNA collection, analysis, storage, and destruction, as well as safeguarding individual rights and privacy [25].

2.2.1. DNA Databases

DNA identification databases refer to a collection of genetic sequence information that is used to identify specific individuals. The following quote provides an example of how DNA databases are defined in criminal procedures legislation:

> *"a database (whether in computerized or other form and however described) containing (a) the following indexes of DNA profiles: a crime scene index, a missing persons index, an unknown deceased persons index, a serious offenders index, a volunteers index, a suspects index, and information that may be used to identify the person from whose forensic material each DNA profile was derived; (b) a statistical index; and (c) any other index prescribed by the regulations* [26]*."*

Large numbers of DNA profiles are collected and stored by law enforcement agencies to aid the investigation of serious crimes. The world's largest forensic DNA databases have been established in the United States and the United Kingdom. In January 2017, the US National DNA Index System (NDIS) contained over 12.5 million offender profiles and 2.6 million arrestee profiles [27]. In March 2017, the UK National DNA Database (NDNAD) contained over 5.2 million individual profiles and over 500,000 crime scene sample profiles [28]. Several countries share DNA profiles internationally when relevant to investigations. For instance, in 2014, the Australian Government acknowledged that it had entered into a DNA profile sharing program with the United Kingdom, the United States and Canada [29].

In Cameroon, the absence of a comprehensive legislation and institutional support specifically governing the collection, storage, and use of DNA evidence in criminal investigations hinders the establishment of a national DNA database and the effective use of DNA evidence in the judicial system. While DNA evidence is occasionally utilized in criminal investigations, its application is limited due to infrastructural and legal constraints. However, law enforcement agencies employ DNA analysis on a case-by-case basis, often relying on public hospitals for testing [30].

2.3. Facial Recognition

Since the nineteenth century, police have used photographs and artist sketches for the purposes of identifying unknown suspects. Facial comparison can be traced back to sketches of suspects in criminal investigations, made by portrait artists on the basis of witness statements [31]. Facial comparison involves the

[22] Butler, J. (2005). Forensic DNA Typing. Burlington, MA: Elsevier.
[23] Smith, M. (2015). DNA Evidence in the Australian Legal System. Sydney: Lexis Nexis.
[24] Law No. 2005 of 27 July 2005
[25] The Forensic DNA Policy Board for Africa's mission is to draft a comprehensive framework for DNA legislation to be adopted by African countries seeking to develop DNA policies. The Board's goal is to enhance the utilisation of forensic DNA profiling in their respective criminal justice systems and for humanitarian purposes. https://www.dnapolicyboard.africa. Accessed on 18/5/2025.
[26] Crimes Act 1914 (Cth), section 23YDAC, Australia.
[27] FBI, 2017.
[28] Home Office, (2017).
[29] Keenan, M. (2014, November 6). Minister signs international DNA exchange pilot with United Kingdom. http://www.ministerjustice.gov.au/Mediareleases/Pages/2014/FourthQuarter/6November2014-MinisterSignsInternationalDNAExchangePilotWithUnitedKingdom.aspx. Accessed on 21/5/2025.
[30] Ibid., 14
[31] Valentine, T. & Davis, J. (2016). Forensic Facial Identification: Theory and Practice of Identification

review of photographic and CCTV images by an expert, where the prosecution seeks to prove that the defendant is the individual depicted. Facial mapping procedures can involve either a quantitative method, where measurements between facial features are compared (photo-anthropometry), or a qualitative method that examines the similarities of facial features (morphological analysis) [32].

There has been a steady expansion of the use of face recognition technology for border control, expediting traveler processing around the world [33]. The most significant application of facial recognition is the potential for integration into Smart CCTV systems. It enables real-time surveillance, identification and tracking of individuals through public places [34].

In the United States, a case of facial recognition used in criminal investigations was presented as evidence at trial. The case involved Charles Heard, who was accused of a murder committed during an armed robbery. The case went to trial in San Francisco in 2010. At trial, the defence sought to have facial recognition results admitted as evidence in an attempt to exculpate the accused, which was allowed by the judge [35]. Surveillance footage of the likely shooter was admitted as evidence, along with testimony from an expert who argued that the images of the shooter were not Charles Heard [36]. Although the jury was unable to agree on the identity of the shooter, Heard was convicted of first-degree murder as it was established that he had participated in the attempted robbery, resulting in the death, and was later sentenced to 25 years imprisonment [37]. In spite of the fact the extent to which the facial recognition evidence influenced the jury's decision-making in this case is unknown, a precedent was set.

Cameroon has expanded its surveillance infrastructure by installing thousands of CCTV cameras equipped with live facial recognition capabilities. These systems are designed to monitor and capture various incidents, including crimes, traffic violations, and other forms of urban disorder, facilitating prompt police intervention. There are also plans to expand facial recognition projects with live surveillance [38]. Despite the technological advancements, Cameroon lacks specific legislation regulating the use of facial recognition technology in criminal investigations. The existing legal instruments, such as the Criminal Procedure Code, provide general guidelines for evidence collection and police procedures but do not address the nuances of biometric surveillance. This absence of a dedicated legal framework means that the deployment and use of facial recognition technology operate without clear standards for data protection, accountability, or oversight. Consequently, there is a risk of potential misuse or abuse of the technology, infringing on individuals' privacy rights and civil liberties.

2.3.1. Databases

There has been an exponential expansion in facial recognition databases around the world. In some cases, police information systems are used as a foundation for facial recognition databases. However, government and law enforcement agencies also routinely access, integrate and search existing databases, such as driver's licence and passport photograph databases. The prior existence of these high-quality digital images has enabled police to form large networks of biometric information that enables the searching of facial images and templates. Unlike DNA or fingerprint databases, these types of facial recognition databases formed from identification documents are comprised of individuals who have not previously been involved in the criminal justice system.

As earlier mentioned, Cameroon has integrated facial recognition technology into its security infrastructure, particularly through extensive CCTV surveillance systems in major urban areas. However, the existence of a centralized facial recognition database specifically for identification and criminal investigations is not clearly documented. In the littoral region, over 3,000 CCTV cameras equipped with facial recognition capabilities have been installed, supported by base stations and command centers to facilitate real-time monitoring and rapid police response. Similarly, the center region operates a video command center with facial recognition features as part of its Smart Cities project, aiming to improve the operational capacity of the

from Eyewitnesses ad CCTV. Chichester: Wiley-Blackwell.

[32] Edmond et al., (2009).

[33] Gold, S. (2014). Biometrics at the border. Biometric Technology Today, October, 5.

[34] Gates, K.A. (2011). Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance. New York: New York University Press.

[35] Jamison, P. (2010, 14 July). Facial profiling: Will face-recognition technology get an accused killer off the hook? SF Weekly. http://archives.sfweekly.com/sanfrancisco/facial-profiling/Content?oid=2177840&storyPage=5. Accessed on 20/5/2025.

[36] Ibid.

[37] Nusca, A. (2011, 1 February). Biometrics valid evidence in trial, judge rules: A San Francisco judge ruled that biometric facial recognition could be submitted as legal evidence in a trial. ZDNet. http://www.zdnet.com/article/biometrics-valid-evidence-in-trialjudge-rules. Accessed on 20/5/2025.

[38] IFSEC INSIDER. Cameroon's largest city switches on live facial recognition video surveillance programme. https://www.ifsecglobal.com/video-surveillance/cameroons-largest-city-switches-on-live-facial-recognition-video-surveillance-programme. Accessed on 19/4/2025.

police to monitor and counter various forms of urban disorder [39]. The legal framework governing the collection, storage, and use of facial recognition data in the country is also not well-defined, raising concerns about oversight, privacy, and civil liberties. However, Cameroon collaborates with international organizations like Interpol to enhance its biometric capabilities. Under Interpol's Project FIRST, biometric data, including facial images, are collected and stored in international databases to aid in identifying individuals involved in transnational crimes [40].

3. INTERNATIONAL GOVERNANCE ON THE USE OF BIOMETRICS FOR CRIME CONTROL

3.1. Human Rights-Compliant use of Biometrics

Resolution 2396 of the Security Council calls upon Member States to assess and investigate suspected foreign terrorist fighters and their accompanying family members, including spouses and children, and to develop and implement comprehensive risk assessments for those individuals [41]. When developing systems to collect biometric data, it is important to put in place safeguards with respect to data protection and human rights standards [42], paying particular attention to the need to ensure that any systems developed to collect and record information, including biometric data, on children are used and shared in a responsible manner, which fully protect children's human rights in accordance with domestic and international law, including, in particular, those listed under the United Nations Convention on the Rights of the Child [43].

The International Covenant on Civil and Political Rights (ICCPR) provides that no one shall be subjected to arbitrary or unlawful interference with his/her privacy, family, home or correspondence, nor to unlawful attacks on his/her honor and reputation; and that everyone has the right to the protection of the law against such interference or attacks. While the right to privacy under international law is not absolute, it is well recognized that any interference with the right must comply with the principles of legality, proportionality and necessity. Moreover, State authorized privacy interference can only take place on the basis of law, which itself must comply with the provisions, aims and objectives of the Covenant, and be reasonable in the particular circumstances [44]. Any such interference must also not constitute discrimination on grounds of race, language, religion, national or social origin, political or other opinion, or any other ground established by international law [45].

The United Nations Special Rapporteur on the right to privacy has noted that several countries around the world have identified an overarching fundamental right to dignity and the free, unhindered development of one's personality, which could be negatively impacted by violations of the right to privacy [46]. The Universal Declaration of Human Rights and the ICCPR begin with their recognition of the inherent dignity and equal and inalienable rights of all members of the human family as the foundation of freedom, justice and peace in the world [47]. These rights could be imperiled by improper use of biometric data. Misuse of such data could also pose serious risks to due-process rights, including the right to the presumption of innocence and other rights connected with criminal proceedings [48]. Furthermore, mass collection of such data without complying with the principles of necessity and proportionality could pose a violation of the right to privacy by itself [49].

3.2. Ethics and Biometrics

The International Organization for Standardization (ISO) has promulgated its standards relating to Jurisdictional and Social Considerations and Commercial Applications, Part 1 General Guidance (ISO/IEC TR 24714:2008) and its Guide 71:2014 which deal with ethics and, in its Guide 71, with accessibility standards for groups such as the aged and disabled.

The ethical use of biometrics extends into the humanitarian domain. The office of the United Nations High Commissioner for Refugees (UNHCR), for example, has used biometric systems in support of its programs since 2002 and increasingly anchors registration in biometrics. UNHCR's global biometric solution, the Biometric Identity Management System (BIMS) allows the organization to ensure the uniqueness of each registration, and to verify that the various forms of assistance the organization may provide (including food, cash, protection or resettlement interventions, among others) are received by the rightful recipients.

The UNHCR also recommends biometric registration of persons applying for asylum as an integral element of protection-sensitive entry systems. This includes instituting proper safeguards to prevent the possible infiltration by criminals or those belonging to terrorist or extremist organizations. Good practices in this regard include: (1) proper registration, including biometrics by border authorities who are trained on relevant aspects of security, refugee and human rights protections; and (2) referral of those who claim

[39] Ibid.
[40] Ibid.,15
[41] UN Security Council Resolution 2396 (2017)
[42] S/2015/975, para. 8; S/2015/939, Principle 15 (e).
[43] United Nations. (1989). Convention on the Rights of the Child.
[44] Human Rights Committee General Comment No. 16: Article 17 (Right to privacy), para 3-4.
[45] ICCPR, Art. 2(1) and 26.
[46] Report of the Special Rapporteur on the right to privacy, A/HRC/31/64 (2016).
[47] Universal Declaration of Human Rights and ICCPR, preamble.
[48] ICCPR, Arts. 9, 14.
[49] ICCPR, Art. 2(3).

international protection to asylum procedures. As a general principle, in order not to place asylum applicants/refugees at risk, their biometric and other personal data should not be shared with their countries of origin, unless the asylum procedure has concluded and protection was not granted. This also applies to third countries in circumstances where effective protection of the asylum claimant or refugee might be put at risk [50].

3.3 Data Protection and the Right to Privacy

3.3.1. Legal Enrolment Criteria and Data Standards

The United Nations Security Council in its resolution 1373 has noted the close connection between international terrorism and transnational organized crime, illicit drugs, money-laundering, illegal arms trafficking. In that same resolution, the Council decided that States shall prevent the movement of terrorists or terrorist groups by effective border controls and controls on issuance of identity papers and travel documents, and through measures for preventing counterfeiting, forgery or fraudulent use of identity papers and travel documents [51]. To counter that relationship, it is critical to develop sufficient and effective counter-terrorist capacity across all member states [52]. The use of biometrics is a vital tool in developing that capacity [53].

In order to implement a biometric system that is both effective and compliant with data protection laws and upholds the right to privacy the following factors need to be considered:

Enrolment Quality Assurance:

High quality enrolment standards must be set so that biometric enrolment and matching can be used accurately in a wide variety of environments such as in remote areas, at established border posts or in airports which are increasingly demanding a more rapid processing of passengers while maintaining accuracy levels. In the case of children or legal minors accompanying parents or travelling alone, due recognition should be paid to the possibility that some biometrics of children can change as they develop. In addition, the UN Security Council in its resolution 2396 stresses that children need to be treated in a manner that observes their rights and respects their dignity, in accordance with applicable international law [54].

Privacy Legislation:

Law enforcement authorities can limit the right to privacy if the measures taken are necessary and proportionate and in compliance with international human rights law. For example, personal data of suspects and associates may be used in emergencies where key privacy principles such as informed consent or the harvesting of related personal data may be set aside. However, those privacy principles such as informed consent, collection and use only for stated purposes and the right to correct inaccurate or misleading records should be treated as the default requirements in the majority of cases. Further, the reasons for deviating from those default requirements should be documented and logged. Operator access to such systems should also be controlled by biometrics to ensure high standards of security.

Financing of Terrorism:

To assist in the prevention of terrorist related fraud, identity theft and financial transactions, biometrics can be used as part of a suite of measures to mitigate such threats across the finance system. The use of biometrics for controlling access to transactions is therefore an effective option. A nationwide program to protect consumers against terrorist-related fraud and identity theft has many benefits at a community and policing level [55].

International Personal Data Standards:

Personal data standards should be set in conformity with international standards rather than using less common modalities or technical standards that may be based on factors such as indigenous industry lobbying or even systems that are provided free by aid donors. The relevant International Organization for Standards (ISO), the International Civil Aviation Organization (ICAO) and World Customs Organization standards should be the initial criteria in system selection, supported by the Biometrics Institute's Privacy Guidelines and Privacy Impact Assessment Checklist [56].

Admissibility of Evidence:

Care should be taken to ensure that the use of all biometric and personal data must be limited to the approved purposes for which it was obtained. This will ensure also that the data collected for databases is admissible for prosecution purposes. This should include provisions to ensure co-operation from the ICT industry provided that a legal basis for such co-operation has been established.

---

[50] See Section E, paragraph 17 of UNHCR "Addressing security concerns without undermining refugee protection" http://www.refworld.org/docid/5672aed34.html. Accessed on 20/4/2025.

[51] S/RES/1373 (2001) Security Council

[52] See also Security Council Resolutions 2195 (2014) and 2178 (2014).

[53] UN Security Council Resolution 2396 (2017) and its previous resolution 2178 (2014).

[54] S/RES/2396(2017) | Security Council

[55] See the International Monetary Fund's website in which anti-laundering and other anti-fraud instruments are listed. www.imf.org. Accessed on 20/4/2025.

[56] See www.biometricsinstitute.org. Accessed on 20/4/2025.

Interpreting Biometric Outputs:

Law enforcement agencies detaining or prosecuting terrorists should be aware of the risks of misinterpreting biometric database results, for example, understanding the value of a partial DNA match or an inconclusive face comparison because of the environmental problems that may occur when a facial image is captured in low quality environments. In those instances, contextual analysis is absolutely essential before any action is taken.

3.3.2. Data Retention or Deletion Policy

This is an area where law enforcement and counter-terrorism procedures must be undertaken in accordance with international human rights law including the right to privacy. For example, the right to see one's file or make corrections or request deletions (which is often guaranteed in privacy legislation, for example, the European Union's *General Data Protection Regulation* GDPR) [57], may also be qualified by the need to protect witnesses or the confidentiality of ongoing investigations.

3.3.3. Data Sharing

The United Nations has stressed, in a number of declarations, the necessity of co-operation between states in terms of legislative improvements to prosecute terrorists, especially foreign terrorist fighters, whilst at the same time, protecting under the law, human rights and privacy [58]. Real-time sharing of personal data such as biometrics both within state authorities and between states also requires co-operation with the aim of harmonizing the inter-operability of platforms and formats [59]. The principles to be followed include: The sharing of personal data, including biometrics, must be lawfully approved domestically and subject to a clear legal framework between the entities sending and receiving the data, domestically and internationally; the use of such data must be limited to the approved purposes for which it was obtained; the data can be shared only with trusted recipients [60].

3.3.4. Data Security and Validation

All effective privacy and security policies and practice require at least the following decisions, regardless of whether or not a biometric has been used: Has a Privacy Impact Assessment [61], been completed before the introduction of a new business practice or new technology? Are there training and awareness programs and procedures that maintain an adequate privacy and human rights culture as well as a working knowledge of biometrics by all personnel operating the system? Are encryption or data reduction techniques used at critical stages of the collection, storage, usage and sharing of personal data including biometrics? Are there rigorous access controls and logging of access which require biometrics to be presented by those accessing sensitive personal data files? Are there documented processes that define the reporting mechanisms and remedial actions required in the event of privacy and security breaches? Are regular tests and audits conducted to ensure that the security and privacy practices are followed and that they are and continue to be robust and effective? Is there a formal process to document and then address issues that become apparent as a result of the regular audit? Are regular, random checks conducted on the validity and integrity of personal data held in the system?

There are a number of international standards and guidelines that provide advice for Data Controllers and their organizations [62]. In terms of validation of the collected data, including biometrics, it is essential that due process is followed in order to protect human rights, including the right to privacy but also to ensure that judicial requirements for convictions or, for example, extradition proceedings are fully complied with. In extradition proceedings, those requirements may be more stringent in some countries than in others, especially in terms of evidentiary and interrogation criteria.

A key guiding principle for law enforcement and border control authorities must be the requirement to have in place dedicated teams of analysts that have the skills and resources to provide actionable and accurate results. This assists pre- and post- incident terrorist

[57] European Union General Data Protection Regulation 2018, Articles 7 (Consent), Article 17 (Right of Erasure), Article 15 (Right of Access to Data)

[58] UN Security Council Resolution 2322 (2016) on international cooperation and UN Security Council Resolution 2396 (2017) Strengthening of Measures to Counter threats Posed by Returning Foreign Terrorists.

[59] UN Security Council Resolution 2178 (2014) and the Madrid Declaration of the Ministers for Foreign Affairs at the special meeting of the Counter-Terrorism Committee of the Security Council 28th July 2015.

[60] Examples of sharing personal data between trusted recipients are the agreements between the UK's ACRO recordable offence data with the US Federal Bureau of Investigations or other European Union police, immigration authorities or INTERPOL'S I-24/7 secure police to police communications system backed up by INTERPOL's Stolen and Lost Travel Documents data base and the Travel Documents Associated with Notices System.

[61] A Privacy Impact Assessment (PIA) forms part of a 'privacy by design' approach to managing data within public and commercial organisations. The PIA process ensures compliance with legal and regulatory requirements for privacy by identifying potential risks and developing mitigation strategies to manage them.

[62] GA Resolution 45/95 (1990) on the Guidelines for the regulation of computerized personal data files and Biometrics Institute's *Biometric Privacy Guidelines* designed for international use www.biometricsinstitute.org. accessed on 20/4/2025.

monitoring and in the acquisition of admissible evidence, including biometrics such as DNA, fingerprints, face and voice. This capability should make full use of all biometric capture and search techniques.

4. INTERNATIONAL STANDARDS

4.1. Technical Operating Standards

The International Organization for Standardization [63]. (ISO) develops and publishes standards across a wide range of industries including biometrics and forensic science. The ISO is a worldwide federation of national standards bodies, from 162 countries, who contribute to the production of standards through membership of the various subject-matter committees. Other countries may join as correspondent or subscriber members to receive information about standards.

ISO also has two joint committees with the International Electrotechnical Commission [64]. (IEC) that sets standards and Conformity Assessments (CA) for all electrical, electronic and related products. A conformity assessment can reassure a prospective purchaser, who may not fully understand the complexities of the system or product, that it meets the required technical and safety standards or other criteria as specified. There are three types of CA. *First Party* CA is conducted by the supplier, *Second Party* CA is carried out by the user but the most robust form of CA, *Third Party*, is conducted by independent bodies. The process is known as Certification because a certificate is usually issued after a successful assessment. Its purpose is to verify that a product or service meets a certain specification or ISO/IEC standard.

Regional bodies may also set standards in order to harmonize the systems and working practices of a group of countries. For example, the European Committee for Standardization [65]. (CEN) brings together the National Standardization Bodies of 34 European countries and has a specific working Group for biometrics (WG18) that adapts standards from international or national organizations to comply with European requirements such as privacy and data protection law.

Some standards are set at the national level by the relevant organization for that country e.g. in the USA there are bodies such as the American National Standards Institute (ANSI) and National Institute of Standards and Technology (NIST) that set standards that apply across forensic science and associated biometric applications. NIST standards have been adopted widely by many countries in key areas such as the electronic transmission of fingerprints across networks. NIST also conducts the competitive testing and ranking of commercially available biometric search and comparison algorithms for other biometric modalities such as faced and iris [66]. This enables prospective buyers of biometric matching systems to obtain objective information regarding the relative performance of the algorithms used by rival manufacturers in the international marketplace.

4.2. Scientific Operating Standards and Quality Management Procedures

In addition to the technical standards and certification programs available for biometric systems there are ISO standards for forensic science procedures such as ISO/IEC 17025:2017 “the general requirements for the competence of testing and calibration laboratories.” This standard addresses the procedures and competencies required to conduct scientific tests and/or calibrations including sampling. It reviews the management of the processes as well as the competence and impartiality of the scientists and the validity of their methods. It uses both internal audits and tests, conducted by the laboratory itself, and external audits and proficiency tests, performed and overseen by external accreditation bodies in order to drive continuous improvement and accredit the laboratory. These regular independent inspections determine if the laboratory meets the required standards to achieve or maintain accreditation under ISO17025:2017. Accreditation confirms that laboratories have a fully operational Quality Management System (QMS) in place and are competent to perform scientific testing and calibration consistently in accordance with the standard.

There are standards that can be applied to other areas of forensic science such as crime scene investigation (e.g. ISO 17020:2012). It is therefore possible and very important to have a standards-based approach in counter terrorism operations that covers all forensic science processes from the crime scene to the courtroom including: Crime scene management and examination including forensic and biometric strategies interpretive assessments, coordination of resources, sampling methods, anti-contamination procedures, packaging materials and the examination of suspects, witnesses and victims.

5. NATIONAL FRAMEWORK ON BIOMETRIC DATA COLLECTION AND STORAGE IN CAMEROON

5.1. Legal Frameworks

The legal framework governing the use of biometrics in crime control in Cameroon involves several laws and regulatory instruments. While Cameroon does not yet have a specific comprehensive biometric law, the use of biometrics in crime control is regulated through a mix of data protection laws, criminal procedure laws, and security regulations.

[63] http://www.iso.org
[64] http://www.iec.ch
[65] https://www.cen.eu
[66] http://www.nist.gov

Cameroon has established a comprehensive legal framework governing the collection, processing, and storage of biometric data through Law No. 2024/017 of 23 December 2024, known as the Personal Data Protection Law. This legislation marks a significant step in aligning Cameroon's data protection standards with international norms. This law applies to both public and private entities that process personal data within Cameroon. It encompasses various forms of personal data, including biometric information such as fingerprints and facial images. The law defines biometric data as personal data resulting from information relating to an individual making it possible to identify him/her directly or indirectly, in particular by reference to any identification number or to one or more factors specific to his/her physical, psychological, genetic, mental cultural, socio-professional or economic identity, in particular a name, a photograph, a fingerprint, a postal address, an email address, a telephone number, a social security number, an internal personal number, a digital identifier, an internet protocol address, a computer connection identifier or a voice recording [67]. Processing biometric data requires explicit consent from the data subject or must be justified by a legal obligation [68]. Transfers of personal data outside Cameroon require prior authorization, ensuring that the recipient country provides adequate data protection [69]. Data controllers and processors are mandated to implement appropriate technical and organizational measures to ensure data security [70]. In the event of a data breach, both controllers and processors must promptly notify the relevant authority and affected individuals [71].

The Cameroonian constitution protects individual privacy, and this protection extends to biometric data. Specifically, the preamble of the constitution guarantees the inviolability of privacy, stating that no interference is allowed except by judicial decision. The constitution further ensures that individuals are not subjected to arbitrary interference with their privacy, including their correspondence [72]. These rights are relevant to the use of biometric data in crime control.

Law N° 2010/012 OF 21 December 2010 Relating to Cybersecurity and Cybercriminality in Cameroon provides a general framework for electronic data protection. It governs the collection, storage, and processing of personal data, which includes biometric data. Article 41–48 cover the protection of personal data and stipulate conditions under which it can be processed, including consent and security measures [73].

The Cameroonian Criminal Procedure Code establishes the general framework for procedural measures in criminal matters, including evidence collection and investigation. While not specifically mentioning biometric data, the code allows for the collection of various types of evidence, including electronic records [74]. This suggests that biometric data, if relevant to an investigation, could potentially be collected under the broader authority granted by the code. The law allows law enforcement agencies to use evidence, including biometric data (fingerprint) in criminal investigations [75]. This provision of the law therefore supports biometric collection for suspects under investigation or prosecution.

5.2. National Institutions and Frameworks

5.2.1. General Delegation for National Security (DGSN)

The DGSN of Cameroon plays a pivotal role in leveraging biometric data to enhance crime control and bolster national security. This initiative is part of a broader strategy to modernize the country's identification systems and improve law enforcement capabilities. As part of its responsibilities, the DGSN oversees the issuance of biometric national identity cards, which incorporate advanced security features such as embedded chips storing fingerprints, facial images, and digital signatures. These cards are designed to prevent identity fraud and are issued within 48 hours of application [76]. The DGSN maintains centralized databases that store biometric information of citizens. These databases facilitate efficient identity verification and aid in criminal investigations by providing law enforcement agencies with reliable data. In collaboration with partners, the DGSN has implemented live facial recognition video surveillance in major cities like Douala, the littoral region of the country. This system uses biometric data to monitor public spaces, detect criminal activities, and enhance urban security [77]. The DGSN utilizes biometric

[67] Section 5 of Law No. 2024/017 of 23 December 2024 Relating to personal data protection in Cameroon.
[68] Ibid. Section 9
[69] Ibid. Section 19.
[70] Ibid. Sections 6, 7, 8 and 15.
[71] Ibid. Section 22
[72] Law No. 96-6 of 18 January 1996 to amend the Constitution of 2 June, 1972 in Cameroon.
[73] LAW N° 2010/012 OF 21 DECEMBER 2010 RELATING TO CYBERSECURITY AND CYBERCRIMINALITY IN CAMEROON
[74] Alongifor Godwin (2024). Appraising the Test of Admissibility of Electronic Records under Cameroonian Criminal Trials. Scholars International Journal of Law, Crime and Justice.
[75] Section 84 of the 2005 Criminal Procedure Code.
[76] SecuringIndustry (2025). Optical technologies: The image of the war on ID counterfeiting. https://www.securingindustry.com/security-documents-and-it/optical-technologies-the-image-of-the-war-on-id-counterfeiting/s110/a16983/?utm_source=chatgpt.com. Accessed on 19/5/2025.
[77] IFSEC GlobaL (2023). Cameroon's largest city switches on live facial recognition video surveillance program. https://www.ifsecglobal.com/video-surveillance/cameroons-largest-city-switches-on-live-

data to strengthen border security. By integrating biometric verification at border checkpoints, the agency aims to prevent illegal crossings and identify individuals involved in transnational crimes [78]. To ensure the effectiveness and security of biometric systems, the DGSN collaborates with international technology providers and organizations. These partnerships facilitate the adoption of best practices and the implementation of cutting-edge biometric technologies [79].

5.2.2. Automated Fingerprint Identification System (AFIS)

Cameroon has integrated AFIS technology into its national identification systems to improve the accuracy and efficiency of identity verification. This system supports the issuance of biometric national ID cards, enabling citizens to access electronic services securely and reducing the risk of identity theft. The AFIS deployment included the enrollment of 20 million records, with a registration throughput of 600 per minute and a deduplication throughput of 50 per minute [80]. Cameroon's law enforcement agencies utilize AFIS to strengthen criminal identification and investigation processes. By digitizing fingerprint records, the system allows for rapid matching of fingerprints found at crime scenes with those in the national database, facilitating the identification of suspects and linking of cases. This technological advancement aids in reducing case backlogs and supports the judiciary with reliable forensic evidence.

5.2.3. National Biometric Identification System

The country has developed a national biometric identification system that integrates various biometric data, such as fingerprints and facial recognition, to create unique profiles for individuals. This system aids in both civil identification and criminal investigations.

5.2.4. Interpol's Project FIRST

Cameroon participates in Interpol's Project FIRST (Facial, Imaging, Recognition, Searching and Tracking), which aims to enhance the capacity of member countries to identify and track individuals involved in transnational crimes and terrorism. Under this initiative, biometric data, including facial images and fingerprints, are collected and shared among participating countries to facilitate cross-border criminal investigations. Under Interpol's Project First, the biometrics of over 500 inmates were captured during a mission in Cameroon and stored in Interpol's database [81].

5.2.5. National Agency for Information and Communication Technologies (ANTIC)

ANTIC plays a pivotal role in Cameroon's efforts to leverage biometric data for crime control. While ANTIC does not directly manage biometric databases like the Automated Fingerprint Identification System (AFIS), it provides essential regulatory, technical, and cybersecurity support that underpins the secure and lawful use of biometric technologies in the country. ANTIC is tasked with regulating and monitoring the security of electronic communication networks and information systems in Cameroon. This includes overseeing electronic certification and ensuring the integrity of digital data, which encompasses biometric information used in various sectors, including law enforcement and civil identification [82].

Under Cameroon's Law No. 2010/012 on cybersecurity and cybercrime, ANTIC is responsible for implementing and enforcing regulations related to electronic security. This legal framework provides the basis for protecting biometric data against unauthorized access and misuse, thereby supporting crime control initiatives that rely on such sensitive information [83].

In terms of capacity building and training, ANTIC actively engages in training programs aimed at enhancing the skills of law enforcement personnel in digital investigation techniques. By equipping officers with the necessary expertise to handle digital evidence, including biometric data, ANTIC contributes to more effective crime detection and prosecution.

facial-recognition-video-surveillance-programme/?utm_source=chatgpt.com. Accessed on 19/5/2025.

[78] The Guardian Post (2024). https://theguardianpostcameroon.com/post/4639/fr/at-opening-of-workshop-in-yaounde-police-boss-stresses-border-control-essential-element-of-internal-security?utm_source=chatgpt.com. Accessed on 19/5/2025.

[79] Ibid., 49

[80] INNOVATRICS. https://www.innovatrics.com/references/national-eid-cards-cameroon/?utm_source=chatgpt.com. Accessed on 19/5/2025.

[81] Biometric update (2022). Interpol program for fighting terrorism through biometrics deployed in Cameroon. https://www.biometricupdate.com/202201/interpol-program-for-fighting-terrorism-through-biometrics-deployed-in-cameroon?utm_source=chatgpt.com. Accessed on 19/5/2025.

[82] Statutory mission of ANTIC. https://www.antic.cm/index.php/en/the-agency/organic-missions.html?utm_source=chatgpt.com. Accessed on 19/5/2025.

[83] Cameroon-Asset Publisher-Octopus Cybercrime Community. https://www.coe.int/en/web/octopus/country-wiki-ap/-/asset_publisher/CmDb7M4RGb4Z/content/cameroon/pop_up?utm_source=chatgpt.com. Accessed on 19/5/2025.

In order to create public awareness and education, the agency organizes seminars and awareness campaigns to educate the public and stakeholders about the importance of cybersecurity and the responsible use of biometric technologies. These initiatives are crucial in fostering a culture of security and privacy, which is essential for the successful implementation of biometric systems in crime control.

6. CONCLUSION

Accurate and reliable identification is an important issue in crime detection. The biometric recognition is emerging as a sound scientific justifiable tool in investigative procedure. The augmentation of wide varieties of criminal activities and advances in biometric technology mean that biometrics will have a more marked impact in crime detection in coming future. While biometric identification systems have significant potential for crime control in Cameroon, their current effectiveness is moderate, hampered by infrastructural, legal, and operational challenges. Strengthening legal frameworks, improving infrastructure, ensuring ethical use, and fostering interagency collaboration are essential steps toward maximizing the benefits of biometric technologies in promoting security and justice.

REFERENCES

- Abercrombie, N. *et al* 1986. *Sovereign Individuals of Capitalism*, London: Alen and Unwin.
- Butler, J. (2005). Forensic DNA Typing. Burlington, MA: Elsevier.
- Caplan, J., and Torpey, J. (eds.) 2001. *Documenting Individual Identity*, Princeton NJ: Princeton University Press.
- Clarke, R. (1994). Human identification in information systems: Management challenges and public policy issues. *Information Technology & People*, *7*(4), 6-37.
- Crimes Act 1914 (Commonwealth Act No. 12 of 1914).
- Edmond, G., Biber, K., Kemp, R. & Porter, G. (2009). Law's looking glass: Expert identification evidence derived from photographic and video images. Current Issues in Criminal Justice 20(3), 337.
- Eugene Arnaud Yombo Sembe. Report on Citizenship Law: Cameroon. RSCAS/GLOBALCIT-CR 2021/13 May 2021.
- *European Union General Data Protection Regulation 2018, Articles 7 (Consent), Article 17 (Right of Erasure), Article 15 (Right of Access to Data)*
- European Union General Data Protection Regulation 2018.
- Federal Bureau of Investigation (FBI). (2017). NDIS Statistics. Retrieved from https://www.fbi.gov/services/laboratory/biometric-analysis/codis/ndis-statistics
- Gates, K.A. (2011). Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance. New York: New York University Press.
- Gold, S. (2014). Biometrics at the border. Biometric Technology Today, October, 5.
- Home Office of the United Kingdom. (2017). National DNA Database Statistics. Retrieved from https://www.gov.uk/government/statistics/national-dna-database-statistics
- Hornung, G., & Roßnagel, A. (2010). An ID card for the internet—The new German ID card with "electronic proof of identity". *Computer, Law & Security Review*, *26*(2), 151-157.
- *Human Rights Committee General Comment No. 16: Article 17 (Right to privacy), para 3-4. International Electrotechnical Commission http://www.iec.ch*
- *International Organization for Standards http://www.iso.org*
- ISO/IEC TR 24714-1:2008, "Information technology -Biometrics - Jurisdictional and societal considerations for commercial applications - Part 1: General guidance."
- ITU (2016). Review of national identity programs. Geneva: International Telecommunication Union(ITU).https://www.google.com/search?q=where+is+ITU&oq=where+is+ITU&aqs=chrome..69i57j0l5.9 868j0j4&sourceid=chrome&ie=UTF-8.
- Jackson, A. & Jackson, J. (2008). Forensic Science (2nd edition), Harlow: Pearson Education.
- Jamison, P. (2010, 14 July). Facial profiling: Will face-recognition technology get an accused killer off the hook? SF Weekly. http://archives.sfweekly.com/sanfrancisco/facial-profiling/Content?oid=2177840&storyPage=5. Accessed on 20/5/2025.
- Jenkins, R. 2004. *Social Identity*, London: Routledge. Jones, R. 2000. Digital Rule.
- Keenan, M. (2014, November 6). Minister signs international DNA exchange pilot with United Kingdom. http://www.ministerjustice.gov.au/Mediareleases/Pages/2014/FourthQuarter/6November2014-MinisterSignsInternationalDNAExchangePilotWithUnitedKingdom.aspx. Accessed on 21/5/2025.
- Kizza, J.M. (2010). Biometrics in: Ethical and social issues in the information age. Texts in Computer Science. Springer, London.
- LAW N° 2010/012 OF 21 December 2010 Relating to Cybersecurity and Cybercriminality in Cameroon
- *Law N°2005 of 27 July 2005 on the CRIMINAL PROCEDURE CODE of Cameroon.*
- Law No. 2024/017 of 23 December 2024 Relating to personal data protection in Cameroon.
- Law No. 96-6 of 18 January 1996 to amend the Constitution of 2 June, 1972 in Cameroon.

- Milne, R. (2013). Forensic Intelligence. Boca Raton, FL: CRC Press.
- Moses, K., Higgins, P., McCabe, M., Probhakar, S. & Swann, S. (2010). Automated fingerprint identification system. In Fingerprint Sourcebook. Washington, DC: National Institute of Justice.
- *National Institute of Standards and Technology (USA) http://www.nist.gov*
- National Science and Technology Council (NTSC). (2006). Privacy and Biometrics: Building a Conceptual Foundation. https://www.hsdl.org/?view&did=463913.
- Nusca, A. (2011, 1 February). Biometrics valid evidence in trial, judge rules: A San Francisco judge ruled that biometric facial recognition could be submitted as legal evidence in a trial. ZDNet. http://www.zdnet.com/article/biometrics-valid-evidence-in-trialjudge-rules. Accessed on 20/5/2025.
- *Report of the Special Rapporteur on the right to privacy, A/HRC/31/64 (2016).*
- Saferstein, R. (2015). Criminalistics: An Introduction to Forensic Science. Harlow: Pearson Education.
- Smith, M. (2015). DNA Evidence in the Australian Legal System. Sydney: Lexis Nexis.
- Tsibong, S. L. (2023). The use of forensic science in the criminal justice system of Cameroon. PhD Thesis within the framework of the doctorate program in Criminology at Selinus University of Sciences and Literature, Italy.
- *UN Security Council Resolutions 1373(2001), 1624 (2005), 2178 (2014), 2195 (2014) and 2396 (2017) & UN General Assembly Resolutions A/RES/68/276 and A/70/L.55*
- *UNHCR "Addressing security concerns without undermining refugee protection" http://www.refworld.org/docid/5672aed34.html*
- United Nations. (1989). Convention on the Rights of the Child.
- *Universal Declaration of Human Rights and ICCPR, preamble. ICCPR, Art. 2(1), 2(3), 9, 14 and 26.*
- Valentine, T. & Davis, J. (2016). Forensic Facial Identification: Theory and Practice of Identification from Eyewitnesses ad CCTV. Chichester: Wiley-Blackwell.
- *Weicheng S and Tieniu T (1999). Automated Biometrics-Based Personal Identification. Proceedings of the National Academy of Sciences of USA, 96(20): 11065-11066.*
- Whiety, E. A., & Hosein, G. (2010). Global identity policies and technology: Do we understand the question? *Global Policy*, *1*(2), 209-215.