

CAMEROON

ACRONYMS

AI	Artificial intelligence
ANTIC	National Agency of ICT
CEMAC	Economic and Monetary Community of Central Africa (from French)
CMC	Cameroon Music Corporation
F.CFA	CFA franc
ICT	Information and communication technology
IMEI	International mobile equipment identity number
IP	Intellectual property
ISP	Internet service provider
NIC	National identity card
SCAAP	Copyright Corporation for Audiovisual and Photography (from French)
SOCADAP	Société civile des droits d’Auteur et droits Voisins des Arts Plastiques et Graphiques
SOCAM	Societe Camerounaise de la Musique
SOCILADRA	Société civile de droits de la littérature et des arts Dramatique
UHC	Universal health coverage
WHO	World Health Organization

MODES OF INFORMED CONSENT

This section provides legal clarity on the modes of informed consent. When data such as genomic data and personal health data are used in health research, clarity is needed on the modes of informed consent (e.g., broad, tiered or open consent) that are legally required from research participants in relation to data collection, analysis, storage, combination, sharing within a jurisdiction, and cross-border sharing.

There is no general data protection legislation. The main applicable tool is the Guide to Good Practices for the Creation, Organization and Operation of Ethics Committees for Human Health in Cameroun. However, this is not binding.

Guide to Good Practices for the Creation, Organization and Operation of Ethics Committees for Human Health in Cameroun

Adults can consent on their own but children need authorisation from a legal representative, including a parent, in order for the consent to be valid. Special provisions are made for incapable people such as detainees and minors.

Scientists should ensure that social and cultural context have been considered while acquiring consent. Moreover, consent should uphold the ethical principles of dignity and autonomy.

Test for validity of free and informed consent

The test for the validity of free and informed consent is that it must be: given prior to any intervention; based on adequate information that the data subject is able to understand; freely given, independent of coercion or undue influence; given clearly; and duly recorded.

The information to be given to participants includes:

- The research activity is aimed at developing scientific knowledge and participation and is not comparable to the administration of a treatment in the framework of a relationship of an individualised doctor/patient.
- The duration of the study and the procedures that will be used.

- The risks and disadvantages associated with their participation in the study.
- Potential benefits for the participants and/or the community, and if there are *no* direct potential benefits this must be clearly stated.
- Alternative treatments that may be available.
- The measures taken to protect the confidentiality of personal data.
- Their right to withdraw from the study at any time without being penalised.
- What to do if the study has negative effects for them.
- Whether they will be compensated if they suffer adverse effects.
- Whether they will be able to continue to benefit from the interventions provided as part of the study once it is completed.

Essential points for evaluation by the Human Health Research Ethics Board

- List all the information that needs to be provided to potential participants.
- Check that all the required information is included in the documents and information materials used.
- Ensure that the information is understandable to the people addressed.
- Assess the methods/procedures used to convey information.
- Assess any constraints that may affect consent.
- Assess the social and cultural context and how it may influence the validity of the consent.

Attention should be paid to the following factors that may compromise the validity of the procedure

- *The social and economic context:* illiteracy and inadequate access to care.
- *The cultural environment:* the role of the community and of the family and various scales of values.
- The asymmetrical nature of the knowledge of researchers and participants, which places participants in a subordinate position.
- The tendency that subjects confuse the fact of participating in research and receiving individualised medical care.

INDIVIDUAL AND COMMUNITY RIGHTS IN GENOMIC DATA

This section provides legal clarity on the nature and content of individual and community rights. Legal clarity is needed on the respective rights of individual research participants and their communities (where appropriate) in genomic data, in particular. These rights potentially include benefit sharing, ownership, and co-ownership in intellectual property rights in discoveries.

Many rights relevant to human genomics research are protected. These include minority and indigenous rights, protection of privacy and all correspondence, and the right to freedom of scientific research. These rights are generally provided for in the Constitution and are further specified in legislation, regulations and policy guidelines.

These laws and policy guidelines apply to research on human diseases and the structure and function of the human body, involving living persons, deceased persons, embryos and foetuses, biological material, and health-related personal data. They outline principles of research on humans to include: the research participant's free and informed consent; respect for human dignity and human rights; the primacy of the beneficial effects of a product over its risks before launching the research project; guarantee of individual responsibility; respect for human vulnerability and personal integrity; and respect for the research participant's privacy and confidentiality.

Regulatory and Supporting Institutions

Several institutions engage in regulating and supporting compliance with human genomic research. These include the:

- International Society of Nephrology
- Ministry of Public Health
- National Ethics Committee for Human Health Research
- Research Ethics Board
- Training and Resources in Research Ethics Evaluation.

Individual and Community Benefit Sharing

The approach to benefit sharing is as follows. First, with respect to research concerning human participants, the research participant must be informed about the purpose, benefits, advantages of and procedures for conducting the research project, its duration, expected constraints and risks, possible medical alternatives, and his/her right to refuse participation or withdraw without any limitation.

Investigators and sponsors of research activities must take the necessary precautions to maximise the benefits and minimise the risks for participants. Research on incapacitated or disabled persons is done only where it has minimal risks and constraints and where research is expected to benefit people with the same condition or disorder. Where a person has no legal capacity to consent, then the intervention of a third party is needed and that intervention must be done for the sole benefit of the individual without the capacity to consent.

Under intellectual property rights, where a patent is granted, the owner becomes the exclusive owner of the patented invention. With benefit sharing, where an invention is made by two or more persons, the right to the patent belongs to them jointly. Therefore, where an invention is made and patented in the name of a community, then the community can share the benefits of that invention.

Benefits

(a) Tissue donation, removal and associated payment

For any tissue, organ, blood or gametes to be removed from a person, that person must give written consent. Where a pregnant woman is asked to donate her embryo or foetus for research, the decision to donate must be based on joint consent of the parents in terms of terminating the pregnancy. Donation of human organs, cells or tissues for financial gain is prohibited. Therefore, the removal of organs or tissue from a living person is meant only for the therapeutic benefit of the recipient. Where research has no direct benefit to the health of the research participant, then

that research activity can be done only if it has acceptable risk and it is an acceptable burden on the research participant.

(b) Patenting

Patenting of inventions is allowed and encouraged. An invention is patentable only when it is new, has inventive steps and has industrial application. However, several inventions are excluded from patenting: discoveries, scientific theories and mathematical methods; inventions having as their subject matter plant varieties, animal species and biological processes for breeding of plants or animals other than microbiological processes and the products of such processes.

DRAFT

GEOSPATIAL DATA FOR PUBLIC HEALTH SURVEILLANCE

This section provides legal clarity on the use of persons’ geospatial data for public health surveillance. Web Geographic Information Systems are increasingly being used in public health surveillance involving infectious diseases. Privacy risks associated with the use of novel geospatial technologies (and the data generated by such technologies) are analysed and legal clarity is provided on how to comply with the law.

The general legal framework in Cameroon is discussed, inclusive of legislation, regulations, and guidelines.

Introduction

Most laws focus on the protection of privacy via the protection of communication, including electronic communications, electronic surveillance and communication networks. However, the Law of Cybersecurity and Cybercrime provides that any electronic communication networks targeted by this law must include satellite, ground and electronic networks used to route electronic communications and audiovisual communication broadcast or distribution networks. The Law also requires subscribers to electronic communication networks to provide their original national identity card with their exact address, including location map and the international mobile equipment identity number (IMEI) of their device. This can be interpreted to include geospatial images and information, collected not only from satellites that are routed electronically as a form of visual communication broadcast, but also provided directly by the individual subscribers. Geospatial data should, in these circumstances, be protected from being unlawfully intercepted. In addition, operators of information systems are required to safeguard the confidentiality of data transported through their communication systems and networks by introducing technical mechanisms to mitigate issues that may negatively affect the functioning, integrity and authentication of such systems, which in turn may negatively affect the confidentiality of data.

Although both the National Digital-Health Strategy and the Health Sector Strategy acknowledge that geographical distribution of diseases is important in their disease prevention strategies and

the geospatial access to healthcare services, neither of these guiding documents deals with the privacy or the confidentiality of data processing aspects of geospatial data.

General Framework

Constitution of the Republic of Cameroon

The Preamble states that the privacy of all correspondence is inviolate. No interference is allowed except by virtue of decisions emanating from judicial power. Furthermore, nobody must be subjected to arbitrary interference with their privacy, family, home or correspondence, nor to attacks on their honour and reputation.

CEMAC Directive No 07/08-UEAC-133-CM-18

This directive sets out the legal framework for the protection of the rights of users of electronic communication services in the CEMAC region. It stipulates that member states must protect the privacy of users by ensuring the confidentiality of their electronic communications. Accordingly, everyone is forbidden from listening to, intercepting or storing communications and data, or enabling such interception or surveillance without the author's consent.

Law No 2010/012 on Cybersecurity and Cybercrime in Cameroon

This Law governs electronic communications in Cameroon and provides that every individual has the right to benefit from electronic communication services no matter where he/she is located in the country. Electronic communications are the emission, transmission or reception of signs, signals, writings, images or sounds by electronic means, and includes email, facsimile transmission, internet, telex, telegraph, telecopy and telephone communication. Participation in an act that violates the secrecy of correspondence or disclosure, publication or use of the content without the authorisation of the sender or recipient is punished.

Though these instruments do not clearly state what is meant by having the right to privacy in the electronic communication sector, the 2013 Decree on consumers' protection in this sector states that the right to privacy entails the confidentiality and respect of the principle of inviolability and secrecy of messages transferred by electronic communication networks, the protection of

consumers' personal data, and the security of information transferred by electronic communication and information systems.

Cybercrime offences and penalties are provided for, including the criminalisation of unlawful interception, illegal access, system interference, misuse of devices, data interference, and computer-related fraud.

Surveillance oversight under the National Agency of ICT (ANTIC)

Judicial authorities have various powers with respect to privacy and data protection. For example, they are empowered to request and access communication data from providers, the conversion of encrypted text, and facilitate and enforce foreign judicial assistance requests. The Law places *surveillance* oversight under the National Agency of ICT (ANTIC) and empowers it to ensure surveillance, detection and information in computer- and cybercrime-related risks. ANTIC is under the technical supervision of the Ministry of Posts and Telecommunications and under the financial supervision of the Ministry of Finance.

Definitions

The Law provides that the electronic communication networks must include satellite, ground and electronic networks when they are used to route electronic communications and audiovisual communication broadcast or distribution networks. Unlawful interception is defined as illegal or unauthorised access to the data of an electronic communications network, an information system, or terminal equipment. Lawful interception is defined as authorised access to the data of an electronic communications network, an information system or terminal equipment without right or authorisation. An electronic communications network is defined as an active or inactive transmission system and, where applicable, switching and routing equipment and other resources that enable signal routing.

Protection of privacy and confidentiality

The Law states that in terms of individual privacy, every individual has the right to the protection of their privacy and judges may take any protective measures, notably sequestration or seizure, to avoid or end the invasion of privacy. Furthermore, confidentiality of information channelled

through electronic communication and information systems networks, including traffic data, must be ensured by operators of electronic communication and network information systems.

Consent requirements

Save for prohibiting any natural person or corporate body from listening to, intercepting, and storing communications and traffic data related to it, there is a consent requirement in further prohibiting the subsection of any such communications to any other means of interception or monitoring *unless the consent of the users concerned has been obtained*. For example, criminal investigation officers can intercept records or transcribe any electronic communication in cases of crime. However, if any personnel of electronic communication network operators or electronic communication service providers receive any requests with regard to the information they control, there must be secrecy.

Privacy Bill

The Bill will govern the collection, processing, transmission, storage, and use of data. The applicable laws mostly cover data relating to electronic communications, while other sectors of activity handle personal data.

Powers of ANTIC

ANTIC ensures, on behalf of the state, the regulation, control and monitoring of activities related to the security of information systems and electronic communication networks. It also helps identify cybercriminals. ANTIC has the power to:

- ensure the ethical use of ICT and protect intellectual property, consumers, public morals, and privacy;
- monitor, detect and provide information on computer risks and the actions of cybercriminals;
- establish material facts in the commission of cybercrime that can be revealed only through systematic, unannounced and pluralist checks carried out by professionals in the sector by judicial police officers and duly commissioned agents; and

- commit its sworn agents who may, as a result, gain access to premises, land or means of transport for professional use, request communication of any professional document and take copies of it, and collect information.

Code of Criminal Procedure, 2007

This Code permits judicial police officers to intercept, record or transcribe any correspondence sent by telecommunication in the event of a crime punishable by imprisonment of at least two years. The magistrate may order the interception, recording and transcription of correspondence transmitted using telecommunications. The interception warrant, which is not subject to appeal, must be in writing, must identify all the elements to intercept, state the offence that motivates the interception, and must be valid for a maximum of four months.

Regulations Identifying the Address or Physical Location of Individuals

Decree No. 2016/375 on the National Identity Card

This Decree establishes a computerised biometric personal National Identity Card (NIC), which contains an electronic chip. The personal data collected includes names, birth date and *place*, gender, height, picture, signature, fingerprints, special signs such as scars or beauty spots on the holder's body, *address*, and parents' names. The biometric NIC is valid for ten years and contains a permanent unique ID number. Law No. 2012/001 on the Electoral Code establishes a permanent biometric personal Voter's Card, which carries the names, date, place of birth, parentage, photo, fingerprints, profession and *address* of the holder.

Decree No. 2015/3759 on the identification of subscribers

This Decree requires that operators of telecommunications networks and ISPs take appropriate measures to ensure the protection, integrity and confidentiality of the *identification data* they hold or process, as well as the information they hold on the *location of customers* subscribed to their networks. It also requires the telecoms regulatory agency to ensure the confidentiality of subscribers' identification data that it accesses. The Decree requires subscribers to provide their original national identity card, *their exact address including location map*, and the *international mobile equipment identity number (IMEI) of their device*. SIM-card registration is in force.

Guidelines

The 2020–2024 National Digital Health Strategic Plan

Digital health will promote Universal Health Coverage (UHC), which will contribute to better patient care and *surveillance of emerging diseases*. Digital health is defined as the use of information and communication technologies (ICTs) in support of health and related fields, including health services, *health surveillance*, health and education literature, knowledge, and health research. The Plan states that by 2024, standards and interoperability components must be developed to improve the collection and exchange of consistent and accurate health *information across geographical and sectoral boundaries*.

The Plan is intended to address key challenges that the health system may face, including geographic inaccessibility, low demand for services, delayed delivery of care, poor adherence to clinical protocols, and costs incurred by individuals.

Health Sector Strategy

This states that there is a need for equity in geographical, financial and cultural access to health services. In Cameroon, health interventions consider both the territorial dimension and the socio-economic and cultural situation of populations (Universal Health Coverage). The Strategy further states that to improve the prevention of oral diseases and visual and hearing disorders, national surveys must be conducted on the prevalence of oral diseases and visual and hearing disorders in order to estimate their magnitude and *geographical distribution* so as to prevent disease. The Strategy also aims to improve the availability and *geographical access* of services for the prevention of vertical transmission of HIV and Hepatitis B from mother to child. It further aims to strengthen the *epidemiological surveillance system*, and strengthen preparedness and response to epidemics and major public health events. *Surveillance systems* will be used to achieve this strategy.

Conclusion and Recommendations

No law deals specifically with geospatial data. The protection of data privacy and confidentiality can be deduced from the broad interpretation of laws relating to electronic communication and the networks that make communication possible.

Cameroon is preparing a Privacy Bill and can learn from the trials of other African countries in instituting similar laws, specifically with regard to dealing with geospatial data in the wake of the Covid-19 pandemic.

DRAFT

CROSS-BORDER SHARING OF DATA

This section reviews the rules as required by data protection law in the cross-border sharing of personal data. The rules on the cross-border sharing of personal data under data protection law do not exist in a vacuum, and therefore other important information that must be followed when sharing personal data is discussed. This information, however, is comprehensive as it relates to the cross-border sharing of personal data.

The relevant national health research regulations as they relate to the cross-border sharing of personal data are reviewed. These national health research regulations set out the required legal and ethical conditions that must be met when processing personal data for research. Applicable national legal and ethical documents are listed, but the discussion only specifies the requirements as they relate to the cross-border sharing of personal data for research. The guide does not treat the legal and ethical requirements generally required for research, and therefore users of this guide must consult with these documents to ascertain these requirements and to ensure that they are met.

The section provides users with a comprehensive description of the requirements to be met in the cross-border sharing of personal data for research. It sets out all the necessary conditions that must be met to legally share data across borders for research.

In countries where no data protection law is in force, the necessary national legal and ethical requirements, as they relate to the cross-border sharing of data, are presented.

The cross-border sharing of data is governed by several legal and ethical regulations, all of which must be met prior to the sharing of data for research. There is no law governing the protection of data in Cameroon, but a data protection Bill is currently being drafted.

Health Research Regulations and Cross-Border Data Sharing

In addition to national laws, several international treaties and conventions have been signed. Of importance in this domain is the African Union Convention on Cyber Security and Personal Data Protection ([the Malabo Convention](#)). Cameroon has also signed but not yet ratified the African Union Convention on Cyber Security and Personal Data Protection.

Law No 2022/008 Relating to Medical Research Involving Human Subjects in Cameroon

This is the relevant national legislation or guidance on the use of data in health research. This Law sets out the legal and ethical requirements that must be met for the conduct of research in Cameroon. Under the legislation, cross-border sharing of data is not defined under the research regulatory frameworks. The legislation states that non-genetic health-related personal data may be disclosed abroad for research purposes if the data subject consents and there is a written data-sharing agreement, a written biological material-sharing agreement, and if a national investigator is involved in the research project.

With regard to genetic data, such data may be exported for research purposes only if the data subject has given his or her free, informed and written consent; the body in charge of ethics establishes that the research cannot be conducted in Cameroon; and a national investigator is involved in the research project.

DRAFT

LEGAL REGULATION OF AI

This section develops/pioneers an approach to the legal regulation of artificial intelligence (AI) in health discovery and innovation. Data science in health research is increasingly used with AI applications that can transform health innovation. This requires robust governance, risk assessment strategies, and mechanisms to protect human rights

There is no specific AI legislation in Cameroon, and no particular legislative provision addresses AI-related issues including predictive algorithms. There is also no technological provision or industry- or sector-specific guidance. It is therefore necessary to consider the legal landscape for AI development and use. Five thematic areas considered most relevant to AI regulation are explored: (1) AI policy documents; (2) Digital/E-Health and medical device regulation; (3) Consumer/ICT Legislation; (4) Data protection law; and (5) Intellectual property.

AI Strategy

Although there is no AI legislation, ongoing initiatives guide the development of AI at national level and the development and use of AI is a priority according to the national development plans. The country has also launched AI strategies, developed AI policies and has reported enacting legislation to address some of the challenges of AI. Cameroon has also launched its first AI training centre through a partnership between state-owned telecommunications operator Camtel and the University of Yaoundé I.

Important strategies are:

- *National Digital Health Strategic Plan 2020–2024*: This stand-alone policy originates from the World Health Assembly Resolution on eHealth, which was endorsed by World Health Organization (WHO) member states and Cameroon. In accordance with the WHO resolution, the Ministry of Public Health and its development partners started drafting the strategic plan. Its implementation is through the relevant departments/agencies of the Ministry of Health and the Ministry of Posts and Telecommunications. The vision is that

by 2024, digital health will effectively contribute to Universal Health Coverage through informed decision-making at all levels of the health pyramid, and through reliable, robust, secure, and interoperable systems. The objective of the strategy is to improve the performance of the health system by optimal use of effective digital technologies at all levels of the health pyramid. Seven principles guide the strategy: (a) continual improvement (maturity model); (b) priority given to interventions with proven effectiveness; (c) patient-centred care; (d) data-based decisions; (e) transparency and accountability; (f) quality assurance; and (g) alignment of interventions by technical and financial partners.

- *Digital Cameroon Strategic Plan 2020*: The strategy highlights the actions to be carried out and appropriate measures to develop ICT uses for the emergence of the digital economy. As an indicator of the digital economy, the strategy indicates that there is an eHealth initiative whereby four Cameroonian hospitals are connected to a telemedicine network and eHealth applications such as the cardiopad and GiftedMoon have been developed to improve access to health services. One of the strategic objectives is to improve the production and supply of digital content. This will be achieved by initiatives that promote the development of the content of e-applications in all sectors of activity (in particular health, tourism, education, transport, agriculture). Another related strategic objective is to ensure digital transformation of administration and companies. To achieve this objective, the strategy identified the need to promote and develop eHealth.

Digital Health/E-Health

Digital Health is guided by the 2020–2024 Digital Strategic Health Plan. No specific legislation addresses software as a medical device in Cameroon. Medical research is regulated by Law No. 2022/008 relating to medical research involving human subjects in Cameroon; Good practice guidelines for the establishment, organisation and operation of research ethics committees for human health, 2016; and Order No. 0977/A/MINSANTE/SESP/SG/DROS/ establishing the

organisation and functioning of human health research ethics committees in structures under the Ministry in charge of Public Health.

Consumer Protection & ICT/E-Legislation

<i>Consumer protection</i>	<ul style="list-style-type: none"> • Law No. 2011/012 on Consumer Protection in Cameroon
<i>ICT/E-legislation</i>	<ul style="list-style-type: none"> • Law No. 2010/013 Regulating Electronic Communications in Cameroon • Law No 2010/021 on Electronic Commerce in Cameroon

Data Protection Law

There is no data protection law. However, legal provisions on data protection are found in several laws covering different fields – especially with respect to electronic communications. It is challenging for users to control the use of their data as some other sectors cover personal data. Cameroon is preparing a Privacy Bill, according to the competent services of the [Ministry of Posts and Telecommunications](#). The Bill will govern the collection, processing, transmission, storage and use of data.

The right to privacy is enshrined in law No 2010/012 Relating to Cyber security and Cyber criminality in Cameroon. Decree No. 2013/0399/PM on the modalities of the consumers' protection in the electronic communication sector provides for the protection of consumer privacy. The provisions of these legal instruments are complemented by those of Law No. 2010/013 Regulating Electronic Communications in Cameroon, which punishes anyone who intercepts and discloses a private conversation without the consent of the author.

Law No. 2022/008 relating to medical research involving human subjects in Cameroon aims to protect persons involved in health research. It protects health-related data.

Intellectual Property

The Bangui Agreement of 1977 as amended

Motivated by the need to promote the effective contribution of IP to development, and to uniformly protect IP in their territory, 15 African states, including Cameroon, concluded the Bangui Agreement. This agreement is the scientific and industrial law of these countries.

Law No 2000/11 on Copyright and Neighbouring rights

Copyright law deals with the rights of intellectual creators and with particular forms of creativity. Copyright is the protection granted to the author of any literary and artistic work. This activity in Cameroon is regulated by Law No 2000/11 on Copyright and Neighbouring rights. Copyright will relate to the expression through which ideas are described, explained and illustrated. It covers the distinctive features of work where it is materially linked to the expression.

All literary or artistic works, irrespective of the mode, worth, genre or purpose of expression, are protected. These include:

a) Protected works

- literary works (expressed in writing) including computer programs;
- musical composition with or without lyrics;
- dramatic, choreographic works and pantomines created for the stage;
- audiovisual works;
- drawings, paintings, lithographs, etchings or wood engravings and other works of the same genre;
- all kinds of sculptures, bas-reliefs and mosaics;
- architectural works, including the drawings, model and the construction;
- tapestries and objects created by the arts and applied arts, including the sketches or patterns and the works themselves;
- maps and graphic and plastic drawings and reproduction of a scientific or technical nature;
- photographic works including works expressed by a process similar to photography.

b) Protected derivative works and collections

The following works are also protected:

- translations, adaptations, arrangements and other transformations/alterations of literary and artistic works and of expressions of folklore;
- collections of works, of expressions of folklore or of simple facts or data, such as encyclopedias, anthologies and databases, whether reproduced on a medium that may be processed by a machine or in any other form, which, by the selection, coordination or arrangement of their contents, constitute creations of the mind.

The protection of the above works will not affect the protection of existing works used in the making of such works.

c) Unprotected works

- ideas in themselves;
- laws, court judgments and other official documents/instruments, including their translations;
- coats of arms, decorations, currency marks and official insignia.

Rights enjoyed under copyright

The owners of copyright in a protected work, but not without regard to the legally recognised rights and interest of others, may exclude others from using it without their authorisation. The author of the creation has exclusive ownership, which is known as copyright. The author also has moral and patrimonial rights.

Duration of copyright

Author patrimonial rights last for his/her lifetime and for 50 years after his/her death. Moral rights have no time limit.

Infringements

The following constitute forgery:

- any exploitation in violation of the law through performance, reproduction, transformation or distribution;

- infringement of the author’s moral rights;
- importation or exportation or sale of forged objects;
- importation or exportation of phonograms or video games produced without the authorisation of their performer or producer where such authorisation is required;
- manufacturing or importing to sell, rent or set up equipment, material, devices or instruments in order to fraudulently record programmes broadcast where such programmes are reserved for a specific public that receives them in return for a fee paid to their operator or his/her legal representatives;
- the fraudulent neutralisation of effective measures used by owners of copyrights or neighbouring rights to protect their works from unauthorised acts;
- allowing the irregular reproduction or performance of protected works;
- failure to pay or unjustified late payment of a fee as provided for by the law;
- carrying out the following acts:
 - unauthorised removal or alteration of any electronic information relating to the copyright regime;
 - distribution, importation for distribution, unauthorised communication of originals or copies of works, performances, videograms, phonograms and programmes, while knowing that the electronic information relating to the copyright regime has been removed or altered without authorisation.

Penalties

The above offences are punishable by 5–10 years of imprisonment or a fine of 500 to 10 million F.CFA or both. The penalties are doubled if the offender is a partner of the owner of the infringed rights. The court may order the confiscation of forged copies, the equipment used to commit the offence and the proceeds derived; the equipment may also be destroyed.

Collective management bodies and their domain of management

The law lays down conditions governing the activities of collective management bodies. Such societies may carry out any act of collective management, such as authorising the use of works, the collection and distribution of royalties, and the judicial defense of rights. There are four

collective management bodies for copyright and neighbouring rights; only one body may be created for each category of copyright and neighbouring rights:

Category A: Literature, dramatic arts, dramatico-musical, choreographic and other similar arts are managed by SOCILADRA (Société civile de droits de la littérature et des arts Dramatique).

Category B: Musical arts are managed by CMC (Cameroon Music Corporation) and this was recently changed to SOCAM (Société Camerounaise de la Musique).

Category C: Audiovisual and photographic art are managed by SCAAP (Copyright Corporation for Audiovisual and Photography).

Category D: Graphic art and fine art are managed by SOCADAP (Société civile des droits d’Auteur et droits Voisins des Arts Plastiques et Graphiques).

Summary and Analysis

Particularly relevant for AI and health research are the National Digital Health Strategic Plan 2020–2024 and the Digital Cameroon Strategic Plan 2020, which aim to leverage information and communication technology for the development of the digital economy and the provision of health services. While there are several policy documents to guide digital health implementation, there is no specific legislation which addresses software as a medical device in Cameroon. The above-mentioned policy documents are interoperable and do not supersede one another. However, relevant provisions in promulgated legislation will take precedence over other regulatory/policy documents.

While Cameroon is developing a Privacy Bill, data protection provisions may be found in current legislation such as that relating to cybercrimes, consumer protection, electronic transactions, and medical research. Those purchasing AI technologies are unlikely to find much protection under Law No. 2011/012 on Consumer Protection in Cameroon. However, ICT/E-legislation, such as Law No 2010/012 Relating to Cyber security and Cyber criminality in Cameroon, Law No. 2010/013 Regulating Electronic Communications in Cameroon, Law No 2010/021 on Electronic Commerce in Cameroon, and a consideration of intellectual property legislation, jurisprudence and soft law may be essential in ensuring that these technologies are properly used.