REPUBLIC OF CAMEROON

PEACE – WORK – HOMELAND

LAW N°2010/012 OF DECEMBER 21, 2010 RELATING ON CYBERSECURITY AND CYBERCRIME IN CAMEROON

FIRST TITLE
GENERAL PROVISIONS

Article 1.- This law governs the security framework for electronic communications networks and information systems, defines and punishes offenses related to the use of information and communication technologies in Cameroon. In this respect, it aims in particular to:

- establish trust in electronic communications networks and information systems; - establish the legal regime for digital evidence and
security activities,
cryptography and electronic certification;
- protect the fundamental rights of natural persons, in particular the right to human dignity, honour and respect for private life, as well as the legitimate interests of legal persons.

Article 2.- Specific applications used in matters of national defense and security are excluded from the scope of this law.

Article 3.- The electronic communications networks covered by this law include: satellite networks, terrestrial networks, electrical networks when they are used for the routing of electronic communications, networks ensuring the broadcasting or distribution of audiovisual communication services.

Article 4.- Within the meaning of this law and its implementing texts, the following definitions are permitted:

1) Illegal access: intentional access, without having the right to do so, to all or part of an electronic communications network, an information system or terminal equipment;

2) Administration responsible for Telecommunications: Ministry or Minister as the case may be, invested on behalf of the Government with general competence over the telecommunications and information and communication technologies sector.

3) Algorithm: sequence of elementary mathematical operations to be applied to data to achieve a desired result;
4) Asymmetric algorithm: encryption algorithm using a public key to encrypt and a private (different) key to decrypt messages;

5) Symmetric algorithm: encryption algorithm using the same key to encrypt and decrypt messages;
6) Active attack: act modifying or altering the resources targeted by the attack (attack on the integrity, availability and confidentiality of data);

7) Passive attack: act that does not alter its target (passive listening, breach of confidentiality);

8) Damage to integrity: intentionally causing a serious disruption or interruption of the operation of an information system, an electronic communications network or terminal equipment, by introducing, transmitting, damaging, erasing, deteriorating, modifying, deleting or making inaccessible data;

9) Security audit: methodical examination of the components and actors of security, policy, measures, solutions, procedures and means implemented by an organization, to secure its environment, carry out compliance checks, assessment checks of the adequacy of the means (organizational, technical, human, financial) invested with regard to the risks incurred, optimization, rationality and performance.

10) Authentication: security criterion defined by a process implemented in particular to verify the identity of a natural or legal person and ensure that the identity provided corresponds to the identity of this person previously registered;

11) Certification Authority: trusted authority responsible for creating and assigning public and private keys as well as electronic certificates;

12) Root Certification Authority: Body entrusted with the mission of accrediting certification authorities, validating the certification policy of accredited certification authorities, and verifying and signing their respective certificates;

13) Electronic certificate: electronic document secured by the electronic signature of the person who issued it and who attests, after verification, the veracity of its content;
14) Qualified electronic certificate: electronic certificate issued by an approved certification authority;
15) Electronic certification: issue of electronic certificate
16) Encryption: a process by which, using a secret convention called a key, clear information is transformed into information that is unintelligible to third parties who do not have knowledge of the key;
17) Key: in an encryption system, it corresponds to a mathematical value, a word, a sentence, which allows, thanks to the encryption algorithm, to encrypt or decrypt a message;
18) Private key: key used in asymmetric encryption mechanisms (or public key encryption), which belongs to an entity and must be secret;

19) Public key: key used to encrypt a message in a system asymmetrical and therefore freely diffused;
20) Secret key: key known to the sender and the recipient used for encrypting and decrypting messages and using the symmetric encryption mechanism;

21) Source code: set of technical specifications, without restriction of access or implementation, of a software or communication, interconnection, exchange protocol or a data format;
22) Audiovisual communication: communication to the public of services of television and sound broadcasting;
23) Electronic communication: emission, transmission or reception of signs, signals, writings, images or sounds, by electromagnetic means;

24) Confidentiality: maintaining the secrecy of information and transactions in order to prevent unauthorized disclosure of information to non-recipients allowing reading, listening, illicit copying of intentional or accidental origin during their storage, processing or transfer;

25) Content: set of information relating to data belonging to natural or legal persons, transmitted or received through electronic communications networks and Information Systems;

26) Illegal content: content that violates human dignity, privacy, honor or national security;
27) Electronic mail: a message, in the form of text, voice, sound or image, sent over a public communications network, stored on a network server or in the recipient's terminal equipment, until the recipient retrieves it;

28) Encryption: use of unusual codes or signals allowing the conversion of information to be transmitted into signals that are incomprehensible to third parties;

29) Cryptanalysis: set of means which makes it possible to analyze previously encrypted information with a view to decrypting it;
30) Cryptogram: Encrypted or coded message;
31) Cryptography: application of mathematics to write information in such a way as to make it unintelligible to those who do not have the ability to decipher it;

32) Cybercrime: all offenses committed through cyberspace by means other than those usually used, and in a manner complementary to traditional crime;

33) Cybersecurity: a set of prevention, protection and deterrence measures of a technical, organizational, legal, financial, human, procedural nature and other actions enabling the achievement of the security objectives set through electronic communications networks, information systems and for the protection of the privacy of individuals;

34) Declaration of certification practices: set of practices (organization, operational procedures, technical and human resources) that the competent certification authority applies in the context of the provision of this service and in accordance with the certification policy(ies) that it has undertaken to respect;

35) Decryption: reverse operation of encryption;
36) Denial of service: attack by saturation of a resource of the information system or the electronic communications network, so that it collapses and can no longer perform the services expected of it;
37) Distributed denial of service: simultaneous attack on the resources of the information system or the electronic communications network, in order to saturate them and amplify the hindering effects;
38) Availability: security criterion enabling the resources of electronic communications networks, information systems or terminal equipment to be accessible and usable as required (the time factor);

39) Electronic signature creation device: set of private encryption equipment and/or software, approved by a competent authority, configured for the creation of an electronic signature;

40) Electronic signature verification device": set of public encryption equipment and/or software, approved by a competent authority, allowing verification by a certification authority of an electronic signature;

41) Data: representation of facts, information or concepts in a form capable of being processed by terminal equipment, including a program enabling the latter to perform a function;
42) Connection data: set of data relating to the access process in an electronic communication;
43) "Traffic data: data relating to an electronic communication indicating the origin, destination, route, time, date, size and duration of the communication or the type of underlying service;

44) Terminal equipment: device, installation or set of installations intended to be connected to an endpoint of an information system and transmitting, receiving, processing or storing information data;

45) Reliability: ability of an information system or a telecommunications network to operate without incident for a sufficiently long time;

46) Provider of electronic communications services: natural or legal person providing services consisting entirely or mainly of the provision of electronic communications;

47) Severity of impact: assessment of the level of severity of an incident, weighted by its frequency of occurrence;
48) Data integrity: security criterion defining the state of an electronic communications network, an information system or terminal equipment which has remained intact and makes it possible to ensure that the resources have not been altered (modified or destroyed) either intentionally or accidentally, so as to ensure their accuracy, reliability and durability;

49) Illegal interception: access without right or authorization to data on an electronic communications network, an information system or terminal equipment;

50) Lawful interception: authorized access to data on an electronic communications network, an information system or terminal equipment

51) Intrusion by interest: intentional and unauthorized access to an electronic communications network or an information system, with the aim of either causing harm or gaining an economic, financial, industrial, security or sovereignty benefit;

52) Intellectual challenge intrusion: intentional and unauthorized access to an electronic communications network or an information system, with the aim of meeting an intellectual challenge that can contribute to improving the performance of the organization's security system;

53) Deceptive software: software that performs operations on a user's terminal equipment without first informing the user of the exact nature of the operations that the software will perform on his terminal equipment or without asking the user if he consents to the software performing these operations;

54) Spyware: a particular type of deceptive software that collects personal information (most visited websites, passwords, etc.) from a user of the electronic communications network;

55) Potentially unwanted software: software that exhibits characteristics of deceptive software or spyware;

56) Clear message": intelligible version of a message and understandable by all ;

57) Cryptographic means: equipment or software designed or modified to transform data, whether information or signals, using secret conventions or to perform an inverse operation with or without a secret convention in order to guarantee the security of the storage or transmission of data, and to ensure their confidentiality and the control of their integrity;

58) Non-repudiation: security criterion ensuring the availability of evidence that can be used against a third party and used to prove the traceability of an electronic communication that has taken place;

59) Certification policy: a set of identified rules defining the requirements with which the certification authority complies in the implementation of its services and indicating the applicability of a certification service to a particular community and/or a class of applications with common security requirements;

60) Security policy: security framework established by an organization, reflecting its security strategy and specifying the means of achieving it;

61) Cryptography service: operation aimed at the implementation, for the account of others, means of cryptography;

62) Electronic communications network: Transmission systems, active or passive, and, where applicable, switching and routing equipment and other resources that enable the routing of signals by cable, radio, optical or other electromagnetic means, including satellite networks, fixed terrestrial networks (with circuit or packet switching, including the Internet) and mobile networks, systems using the electrical network, insofar as they are used for the transmission of signals, networks used for sound and television broadcasting and cable television networks, regardless of the type of information transmitted;

63) Telecommunications network: installation or set of installations ensuring either the transmission and routing of telecommunications signals, or the exchange of control and management information associated with these signals between the points of this network; 64) Security: situation in which someone or something is not exposed to any danger. Mechanism intended to prevent a harmful event, or to limit its effects;

65) Certification service: service provided by a certification authority certification;

66) Electronic communications service: service consisting entirely or mainly of the provision of electronic communications excluding the contents of audiovisual communications services;

67) Signatory: natural person, acting on his own behalf or on behalf of the natural or legal person he represents, who uses an electronic signature creation device;

68) Electronic signature: signature obtained by an asymmetric encryption algorithm allowing the sender of a message to be authenticated and its integrity to be verified;

69) Advanced electronic signature: electronic signature obtained at using a qualified electronic certificate;

70) Open standard: communication, interconnection or exchange protocol and interoperable data format, the technical specifications of which are public and without restriction of access or implementation;

71) Detection system: system for detecting incidents that could lead to violations of the security policy and for diagnosing potential intrusions;

72) Information system: isolated device or group of interconnected or related devices, ensuring by itself or by one or more of its elements, in accordance with a program, automated processing of data;

73) Vulnerability: a security flaw resulting either intentionally or accidentally in a violation of the security policy, in

the architecture of an electronic communications network, in the design of an information system.

Article 5.- The terms and expressions not defined in this law retain their definitions or meanings given by the international legal instruments to which the State of Cameroon has subscribed, in particular, the Constitution and the Convention of the International Telecommunications Union, the Radio Regulations and the International Telecommunications Regulations.

TITLE II
CYBERSECURITY

CHAPTER I
OF THE GENERAL ELECTRONIC SECURITY POLICY

Article 6.- The Administration responsible for Telecommunications develops and implements the electronic communications security policy, taking into account technological developments and the Government's priorities in this area.

In this capacity, she:

- ÿ ensures the promotion of the security of electronic communications networks and information systems as well as monitoring the development of issues related to security and certification activities;
- ÿ coordinates at the national level activities contributing to the security and protection of electronic communications networks and information systems;
- ÿ ensures the establishment of an adequate framework for the security of electronic communications;
- ÿ establishes the list of certification authorities;
- ÿ ensures the representation of Cameroon in international bodies responsible for activities related to the security and protection of electronic communications networks and information systems.

CHAPTER II
ON THE REGULATION AND MONITORING OF ELECTRONIC SECURITY ACTIVITIES

Article 7.- (1) The National Agency for Information and Communication Technologies, hereinafter referred to as the Agency, established by the law governing electronic communications in Cameroon, is responsible for the regulation of electronic security activities, in collaboration with the Telecommunications Regulatory Agency.

(2) The Agency provided for in paragraph 1 above, ensures, on behalf of the State, the regulation, control and monitoring of activities related to the security of information systems and electronic communications networks, and to electronic certification. In this capacity, its missions include in particular:

- to process accreditation applications and prepare the specifications of the certification authorities and submit them for signature to the Minister responsible for Telecommunications;

- to check the conformity of electronic signatures issued;

ÿ to participate in the development of the national policy on the security of electronic communications and certification networks; ÿ to issue an advisory opinion on texts relating to its field of skill ;

- to monitor the security activities of electronic communications networks, information and certification systems;

- to process applications for approval of cryptographic means and to issue approval certificates for security equipment;

ÿ to prepare mutual recognition agreements with foreign parties and submit them for signature to the Minister responsible for Telecommunications;

- to ensure technological monitoring and issue alerts and recommendations regarding the security of electronic communications networks and certification;

ÿ to participate in research, training and study activities relating to the security of electronic communications networks, information systems and certification;

- to ensure the regularity and effectiveness of information systems security audits in accordance with relevant standards of public bodies and certification authorities;

ÿ to ensure monitoring, detection and information on IT and cybercrime risks;

- to carry out any other mission of general interest that may be entrusted to it the supervisory authority.

(3) A decree of the Prime Minister specifies the methods of application of the provisions of paragraph 1 above.

Article 8.- (1) The Agency is the Root Certification Authority.

(2) The Agency is the certifying authority of the Administration Public.

Article 9.- (1) Accredited certification authorities, security auditors, security software publishers and other approved security service providers are subject to the payment of a contribution of 1.5% of their turnover excluding tax, intended to finance a fund called the “Special Fund for Electronic Security Activities”, for the financing of research, development, training and studies in the field of cybersecurity.

(2) The resources referred to in paragraph 1 above are recovered by the Agency and deposited in an account opened at the Central Bank.

(3) A Committee is hereby established to validate priority research, development, training and study projects in cybersecurity.

The operating procedures of this Committee are set out in a regulatory text.

(4) The Minister responsible for Telecommunications is the authorising officer for expenditure incurred from the fund referred to in paragraph 1 above.

(5) The conditions and methods of collecting and managing this fee are defined by regulation.

CHAPTER III
ON THE LEGAL REGIME OF CERTIFICATION ACTIVITIES

Article 10.- Electronic certification activity is subject to prior authorization. It is carried out by certification authorities.

Article 11.- The following may be subject to authorization:

- ÿ the establishment and operation of an infrastructure for the purpose of issuing, storing and delivering qualified electronic certificates;
- ÿ making available to the public the public keys of all users.

Article 12.- The conditions and procedures for granting the authorization referred to in Article 10 above are set by regulation.

CHAPTER IV
SECURITY ACTIVITIES

Article 13.- (1) Electronic communications networks and information systems, operators, certification authorities and providers of electronic communications services are subject to a mandatory security audit.

(2) The conditions and procedures for the security audit provided for in paragraph 1 above are defined by regulation.

Article 14.- The Agency's staff and experts appointed to carry out audit operations are bound by professional secrecy.

CHAPTER V
OF ELECTRONIC CERTIFICATION

Article 15.- (1) Qualified electronic certificates are only valid for the purposes for which they were issued.

(2) The devices for creating and verifying qualified certificates are technologically neutral, standardized, approved and interoperable.

Article 16.- (1) Certification authorities are liable for damage caused to persons who have relied on certificates presented by them as qualified in each of the following cases:

- ÿ the information contained in the certificate, on the date of its issue, were inaccurate;
- ÿ the data required for the certificate to be considered as qualified were incomplete;
- ÿ the issue of the qualified certificate did not give rise to verification that the signatory holds the private agreement corresponding to the public agreement of this certificate;
- ÿ the certification authorities and certification providers have not, where applicable, registered the revocation of the qualified certificate and made this information available to third parties.

(2) Certification authorities shall not be liable for damage caused by use of the qualified certificate exceeding the limits set for its use or the value of the transactions for which it may be used, provided that these limits are included in the qualified certificate and are accessible to users.

(3) Certification authorities must provide evidence of sufficient financial security, specifically allocated to the payment of sums they may owe to persons who have reasonably relied on the qualified certificates they issue, or insurance covering the financial consequences of their professional civil liability.

CHAPTER VI
OF THE ELECTRONIC SIGNATURE

Article 17.- The advanced electronic signature has the same legal value as the handwritten signature and produces the same effects as the latter.

Article 18.- An advanced electronic signature must meet the following conditions:

- ÿ the data relating to the creation of the signature are linked exclusively to the signatory and are under his exclusive control;
- ÿ any modification made to it is easily detectable;

- it is created using a secure device whose technical characteristics are set out in a text from the Minister responsible for Telecommunications;

ÿ the certificate used to generate the signature is a qualified certificate. A text from the Minister responsible for Telecommunications sets out the qualification criteria for certificates.

CHAPTER VII
ELECTRONIC CERTIFICATES AND SIGNATURES ISSUED BY THE CERTIFICATION AUTHORITIES

Article 19.- The certification authority having conferred validity on an electronic certificate cannot renounce it.

Article 20.- (1) An electronic certificate issued outside the national territory produces the same legal effects as a qualified certificate issued in Cameroon provided that there is an act of recognition of the issuing authority signed by the Minister responsible for Telecommunications.

(2) The interoperability of qualified electronic certificates is regulated by a text from the Minister responsible for Telecommunications.

CHAPTER VIII
OF THE ELECTRONIC DOCUMENT

Article 21.- Any person wishing to affix their electronic signature to a document may create this signature using a reliable device whose technical characteristics are set out in a text from the Minister responsible for Telecommunications.

Article 22.- Any person using an electronic signature device must:

- take the minimum precautions set out in the text referred to in Article 21 above, in order to avoid any illegal use of the encryption elements or personal equipment relating to its signature;

- inform the certification authority of any illegitimate use of its signature;

- ensure the veracity of all data that it has declared to the electronic certification service provider and to any person to whom it has asked to rely on its signature.

Article 23.- In the event of failure to comply with the commitments provided for in Article 22 above, the holder of the signature is liable for any damage caused to others.

CHAPTER IX
ON THE PROTECTION OF ELECTRONIC COMMUNICATIONS NETWORKS, INFORMATION SYSTEMS AND PERSONAL PRIVACY

SECTION I
ON THE PROTECTION OF ELECTRONIC COMMUNICATIONS NETWORKS

Article 24.- Operators of electronic communications networks and providers of electronic communications services must take all necessary technical and administrative measures to guarantee the security of the services offered. To this end, they are required to inform users:

- the danger incurred in the event of use of their networks;
- specific risks of security breaches, including distributed denial of service, abnormal rerouting, traffic spikes, unusual traffic and ports, passive and active eavesdropping, intrusions and any other risk;
- the existence of technical means to ensure the security of their communications.

Article 25.- (1) Network operators and providers of electronic communications services have the obligation to retain connection and traffic data for a period of ten (10) years.

(2) Network operators and electronic communications service providers shall install mechanisms for monitoring data traffic on their networks. This data may be accessible during judicial investigations.

(3) The liability of network operators and providers of electronic communications services is incurred if the use of data provided for in paragraph 2 above infringes the individual freedoms of users.

SECTION II
ON THE PROTECTION OF INFORMATION SYSTEMS

Article 26.- (1) Information system operators shall take all technical and administrative measures to ensure the security of the services offered. To this end, they shall equip themselves with standardized systems enabling them to identify, evaluate, process and continuously manage the risks linked to the security of information systems in the context of the services offered directly or indirectly.

(2) Information system operators shall implement technical mechanisms to deal with attacks detrimental to the permanent availability of the systems, their integrity, their authentication, their non-repudiation by third-party users, the confidentiality of data and physical security.

(3) The mechanisms provided for in paragraph 2 above are subject to approval and proper visa by the Agency.

(4) Information system platforms are protected against possible radiation and intrusions which could compromise the integrity of the transmitted data and against any other external attack, in particular by an intrusion detection system.

Article 27.- Legal entities whose activity is to provide access to information systems are required to inform users:

- the danger involved in the use of information systems unsecured, especially for individuals;
- the need to install parental control devices;
- specific risks of security breaches, in particular the generic family of viruses;

- the existence of technical means to restrict access to certain services and to offer them at least one of these means, in particular the use of the most recent operating systems, antivirus tools and tools against spyware and deceptive software, the activation of personal firewalls, intrusion detection systems and the activation of automatic updates.

Article 28.- (1) Operators of information systems shall inform users of the prohibition on using the electronic communications network to disseminate illegal content or any other act which may undermine the security of networks or information systems.

(2) The prohibition also covers the design of deceptive software, spyware, potentially unwanted software or any other tool leading to fraudulent behavior.

Article 29.- (1) Operators of information systems are required to retain the connection and traffic data of their information systems for a period of ten (10) years.

(2) Operators of information systems are required to install monitoring mechanisms to control access to data in their information systems. The stored data may be accessible during judicial investigations.

(3) The installations of information systems operators may be subject to search or seizure by order of a judicial authority under the conditions provided for by the laws and regulations in force.

Article 30.- (1) Information systems operators shall evaluate, review their security systems and, where necessary, introduce appropriate changes to their security practices, measures and techniques in line with technological developments.

(2) Operators of information systems and their users may cooperate with each other in the development and implementation of security practices, measures and techniques for their systems.

Article 31.- (1) Providers of content in electronic communications networks and information systems are required to ensure the availability of content, as well as that of data stored in their facilities.

(2) They have an obligation to implement filters to deal with harmful attacks on personal data and the privacy of users.

Article 32.- (1) Electronic communications networks and information systems are subject to a mandatory and periodic security audit regime of their security systems by the Agency.

(2) The safety audit and severity impact measurements are carried out annually or when circumstances require.

(3) Audit reports are confidential and addressed to the Minister responsible for Telecommunications.

(4) A text from the Minister responsible for Telecommunications sets out the conditions for assessing the severity impact levels.

SECTION III
OBLIGATIONS OF ACCESS, SERVICE AND CONTENT PROVIDERS

Article 33.- Persons whose activity is to offer access to electronic communications services shall inform their subscribers of the existence of technical means enabling them to restrict access to certain services or to select them and shall offer them at least one of these means.

Article 34.- (1) The liability of persons who ensure, even free of charge, the storage of signals, writings, images, sounds or messages of any nature provided by the recipients of these services, may be incurred.

(2) However, the liability provided for in paragraph 1 above is not point engaged in the following cases:

- the persons did not actually have knowledge of their illicit nature or of facts and circumstances revealing this nature;

- if, from the moment they became aware of the facts, they acted promptly to remove this data or make access to it impossible.

Article 35.- (1) The persons mentioned in Articles 33 and 34 above are required to keep, for a period of ten (10) years, data allowing the identification of any person having contributed to the creation of the content of the services of which they are providers.

(2) They provide persons who publish an electronic communications service with technical means enabling them to satisfy the identification conditions provided for in Articles 37 and 38 below.

(3) The judicial authority may request communication from the service providers mentioned in Articles 33 and 34 above of the data provided for in paragraph 1 above.

Article 36.- The competent court seized shall rule within a maximum period of thirty (30) days on all measures likely to prevent damage or to put an end to damage caused by the content of an electronic communications service.

Article 37.- Persons whose activity consists of publishing an electronic communications service, make available to the public:

- their surname, first names, address and telephone number and, if they are subject to the formalities of registration in the trade and personal property register, their registration number, if they are natural persons;

- their name or business name and registered office, their telephone number and, if they are legal entities subject to the formalities of registration in the trade and personal property register, their registration number, their share capital, the address of their registered office, if they are legal entities;

- the name of the director or co-director of the publication and, where applicable where applicable, that of the editorial manager;
- the name, denomination or business name, address and telephone number of the service provider mentioned in Articles 33 and 34.

Article 38.- (1) Persons publishing an electronic communications service on a non-professional basis may only make available to the public the name, denomination or business name and address of the provider.

(2) The persons mentioned in Articles 33 and 34 above are subject to professional secrecy.

Article 39.- (1) Any person who is the victim of defamation by means of an electronic communications service has a right of reply and may demand that it be rectified.

(2) The conditions for inclusion of the right of reply are those provided for by the texts in force.

Article 40.- (1) Any person carrying out an activity of transmitting content on an electronic communications network or providing access to an electronic communications network may only be held liable when:

- it is the origin of the disputed transmission request;

- it selects or modifies the contents which are the subject of the transmission.

(2) Any person carrying out, for the sole purpose of making their subsequent transmission more efficient, an activity of automatic, intermediate and temporary storage of the content that a service provider transmits, cannot be held civilly or criminally liable for this content unless they have modified this content, have not complied with their conditions of access and the usual rules concerning their updating or have hindered the lawful and usual use of the technology used to obtain the data.

SECTION IV
ON THE PROTECTION OF THE PRIVACY OF INDIVIDUALS

Article 41.- Everyone has the right to respect for their private life. Judges may take precautionary measures, including sequestration and seizure, to prevent or stop an invasion of privacy.

Article 42.- The confidentiality of communications routed through electronic communications networks and information systems, including traffic data, is ensured by the operators and managers of electronic communications networks and information systems.

Article 43.- The content provider is responsible for the content conveyed by its information system, particularly when this content infringes on human dignity, honour and privacy.

Article 44.- (1) Any natural or legal person is prohibited from listening to, intercepting, storing communications and related traffic data, or subjecting them to any other means of interception or surveillance, without the consent of the users concerned, except when that person is legally authorized to do so.

(2) However, technical storage prior to the routing of any communication is authorized for operators and operators of electronic communications networks, without prejudice to the principle of confidentiality.

Article 45.- The recording of communications and related traffic data, carried out in a professional context with a view to providing digital proof of an electronic communication is authorized.

Article 46.- (1) Providers of content for electronic communications networks and information systems are required to retain the content and data stored in their facilities for a period of ten (10) years.

(2) Providers of content for electronic communications networks and information systems are required to implement filters to deal with harmful attacks on personal data and the privacy of users.

Article 47.- The use of electronic communications networks and information systems for the purpose of storing information or accessing information stored in terminal equipment of a natural or legal person may only be done with their prior consent.

Article 48.- (1) The transmission of electronic messages for prospecting purposes by concealing the identity of the sender in whose name the communication is made, or without indicating a valid address to which the recipient can send a request to obtain the cessation of this information is prohibited.

(2) Sending electronic messages by impersonating of others is prohibited.

SECTION V
INTERCEPTION OF ELECTRONIC COMMUNICATIONS

Article 49.- Notwithstanding the provisions of the Code of Criminal Procedure, in the event of crimes or offenses provided for in this law, the Judicial Police Officer may intercept, record or transcribe any electronic communication.

Article 50.- If operators of electronic communications networks or providers of electronic communications services encode, compress or cipher the transmitted data, the corresponding interceptions are provided in clear text to the services which requested them.

Article 51.- The personnel of operators of electronic communications networks or providers of electronic communications services are bound by professional secrecy with regard to the requisitions received.

TITLE III
CYBERCRIME

CHAPTER I
PROVISIONS OF PROCESSUAL LAW

Article 52.- (1) In the event of a cyber offense, the Judicial Police Officers with general jurisdiction and the authorized agents of the Agency shall carry out investigations in accordance with the provisions of the Code of Criminal Procedure.

(2) Before taking up their duties, the authorized agents of the Agency shall take an oath before the competent Court of First Instance, in the following form: "I swear to faithfully fulfill my duties and to observe in all respects the duties imposed upon me, and to keep secret the information of which I have become aware during or in the exercise of my duties."

(3) Judicial Police Officers and authorized agents of the Agency may, during investigations, access means of transport, any premises used for professional purposes, excluding private homes, in order to search for and note offenses, request the communication of all professional documents and take copies thereof, and collect, upon summons or on site, information and justifications.

Article 53.- (1) Searches in cybercrime matters may involve data which may be physical media or copies made in the presence of persons attending the search.

(2) When a copy of the seized data has been made, it may be destroyed on the instructions of the Public Prosecutor for security reasons.

(3) With the agreement of the Public Prosecutor, only objects, documents and data used to establish the truth will be kept under seal by the Judicial Police Officer.

(4) Persons present during the search may be required to provide information on the objects, documents and data seized.

Article 54.- Searches and seizures are carried out in accordance with the provisions of the Code of Criminal Procedure, taking into account the deterioration of evidence.

Article 55.- (1) When it appears that the data seized or obtained during the investigation or inquiry have been subject to transformation operations preventing access to the unencrypted version or are likely to compromise the information they contain, the Public Prosecutor, the Examining Magistrate or the trial court may requisition any qualified natural or legal person to carry out the technical operations enabling the unencrypted version of said data to be obtained.

(2) Where a means of cryptography has been used, the judicial authorities may require the secret agreement for decrypting the cryptogram.

Article 56.- The requisition provided for in Article 50 above may be made to any expert. In this case, its execution is carried out in accordance with the provisions of the Code of Criminal Procedure relating to the commission of experts.

Article 57.- (1) The Cameroonian judicial authorities may issue a national or international letter of request to any legal or natural person to search for the constituent elements of cybercrime offences, at least one of the constituent elements of which was committed on Cameroonian territory or one of the perpetrators or accomplices of which is located in the said territory.

(2) Subject to the rules of reciprocity between Cameroon and foreign countries bound by a judicial cooperation agreement, letters rogatory are executed in accordance with the provisions of the Code of Criminal Procedure.

Article 58.- (1) Natural or legal persons who provide cryptography services aimed at ensuring a confidentiality function are required to provide the Judicial Police Officers or authorized agents of the Agency, upon their request, with the agreements allowing the decryption of data transformed by means of the services they have provided.

(2) The Judicial Police Officers and authorized agents of the Agency may request the providers of the services referred to in paragraph 1 above to implement these agreements themselves, unless they demonstrate that they are unable to meet such requests.

Article 59.- (1) When justified by the requirements of the investigation or the investigation, the hearing or interrogation of a person and/or the confrontation between several persons may be carried out at several points in the national territory which are connected by electronic means of communication guaranteeing the confidentiality of the transmission. A report of the operations carried out there shall be drawn up in each of these places. These operations may be subject to audiovisual and/or sound recording.

(2) Where circumstances so require, interpretation may be provided during a hearing, interrogation or confrontation by electronic means of communication.

(3) The provisions of this article are also applicable for the simultaneous execution, at a point in the national territory and at a point located outside, of requests for mutual assistance from foreign judicial authorities or acts of mutual assistance carried out abroad at the request of the Cameroonian judicial authorities.

(4) The terms of application of this article are defined by regulatory route.

CHAPTER II
OFFENSES AND SANCTIONS

Article 60.- (1) When a certification authority does not comply with the obligations to which it is subject, the Agency may, after having formally notified the structure to submit its observations, order a ban on the circulation of the means of cryptography concerned.

(2) The ban on placing on the market is applicable throughout the national territory. It also imposes on the supplier the obligation to withdraw:

- means of cryptography whose circulation has been prohibited with commercial broadcasters;
- materials constituting means of cryptography whose circulation has been prohibited and which have been acquired for a fee, directly or through commercial distributors.

(3) The cryptographic means concerned may be put back into circulation as soon as the previously unfulfilled obligations have been met and duly noted by the Agency.

Article 61.- (1) Agency personnel and experts of legal entities responsible for audits who reveal, without authorization, confidential information of which they became aware during a security audit shall be punished by imprisonment of three (03) months to three (03) years and a fine of 20,000 (twenty thousand) to 100,000 (one hundred thousand) CFA francs.

(2) Is punishable by imprisonment of three (03) months to four (04) years, the refusal to comply with summonses from authorized agents of the Agency.

(3) Anyone who, by any means whatsoever, obstructs, incites resistance or prevents the conduct of the security audits provided for in this article or refuses to provide the information or documents relating thereto shall be punished with imprisonment of one (01) to five (05) years and a fine of 100,000 (one hundred thousand) to 1,000,000 (one million) CFA francs or one of these two penalties only.

Article 62.- (1) Anyone who presents to the persons mentioned in Articles 33 and 34 above, content or an activity as being illicit with the aim of obtaining its withdrawal or stopping its dissemination, while knowing this information to be inaccurate, shall be punished with imprisonment of one (01) to five (05) years and a fine of 200,000 (two hundred thousand) to 2,000,000 (two million) CFA francs.

(2) The publication director is required to insert, under penalty of a fine of 100,000 (one hundred thousand) to 2,000,000 (two million) CFA francs, within forty-eight (48) hours of their receipt, the responses of any person designated in the electronic communications service.

Article 63.- (1) The legal or de facto manager of a legal entity carrying out the activity defined in Articles 33 and 34 of this law, who has not kept the information referred to in Articles 25 and 29 above, shall be punished with imprisonment of one (01) to five (05) years and a fine of 40,000 (forty thousand) to 4,000,000 (four million) CFA francs.

(2) The de jure or de facto manager of a legal person carrying out the activity defined in Articles 37 and 38 who does not comply with the requirements set out in said Articles shall be liable to the same penalties.

Article 64.- (1) Legal persons are criminally liable for offences committed on their behalf by their governing bodies.

(2) The criminal liability of legal persons does not exclude that of natural persons who are perpetrators or accomplices of the same acts.

(3) The penalties incurred by legal persons are fines of 5,000,000 (five million) to 50,000,000 (fifty million) CFA francs.

(4) Notwithstanding the penalty provided for in paragraph 3 above, one of the following additional penalties may also be imposed on legal persons:

- dissolution when it concerns a crime or an offense punishable with regard to natural persons by a prison sentence greater than or equal to three (03) years and when the legal person has been diverted from its object to serve as a support for the commission of the incriminated acts;

- the prohibition, permanently or for a period of at least five years, from exercising directly or indirectly one or more professional or social activities;

- the temporary closure for a period of at least five (05) years, under the conditions provided for by article 34 of the Penal Code, of the establishments or one or more of the establishments of the company used to commit the incriminated acts;
- exclusion from public markets permanently or for a period of at least five (05) years;
- the ban, permanently or for a period of five (05) years less, to make a public appeal for savings;
- the prohibition, for a period of at least five (05) years, of issuing checks other than those which allow the withdrawal of funds by the drawer from the drawee or those which are certified or of using payment cards; - the confiscation of the thing which was used or was intended to commit the offense or of the thing which is the product thereof; - the publication or dissemination of the decision pronounced either by the written press or by any means of communication to the public by electronic means.

Article 65.- (1) Anyone who, without right or authorization, intercepts by technical means data during transmission or not, to, from or within an electronic communications network, an information system or terminal equipment, shall be punished with imprisonment of five (05) to ten (10) years and a fine of 5,000,000 (five million) to 10,000,000 (ten million) CFA francs or one of these two penalties only.

(2) Any unauthorized access to all or part of an electronic communications network or an information system or terminal equipment shall be punishable by the penalties provided for in paragraph 1 above.

(3) The penalties provided for in paragraph 1 above are doubled in the event of unlawful access affecting the integrity, confidentiality or availability of the electronic communications network or the information system.

(4) Any person who, without authority, allows access to an electronic communications network or to an information system by intellectual challenge shall be punished with the same penalties provided for in paragraph 1 above.

Article 66.- (1) Anyone who causes the disruption or interruption of the operation of an electronic communications network or terminal equipment by introducing, transmitting, damaging, erasing, deteriorating, modifying, deleting or making data inaccessible shall be punished with imprisonment of two (02) to five (05) years and a fine of 1,000,000 (one million) to 2,000,000 (two million) CFA francs or one of these two penalties only.

(2) Persons who use misleading or undesirable software to carry out operations on a user's terminal equipment without first informing the user of the exact nature of the operations that the said software is likely to damage shall be liable to the same penalties provided for in paragraph 1 above.

(3) Anyone who, using potentially unwanted software, collects, attempts to collect or facilitates one of these operations to access information from the operator or provider of a network or electronic service in order to commit offenses shall be punished with the same penalties provided for in paragraph 1 above.

Article 67.- Constitutes an attack on the integrity of an electronic communications network or an information system and is punishable by the penalties provided for in Article 66, paragraph 1 above, the act of causing a serious disruption or interruption of the operation of an electronic communications network of terminal equipment by the introduction, transmission, modification, deletion or alteration of data.

Article 68.- (1) Anyone who fraudulently accesses or maintains access to all or part of an electronic communications network or an information system by transmitting, damaging, causing serious disruption or interruption of the operation of said system or network shall be punished with imprisonment of five (05) to ten (10) years and a fine of 10,000,000 (ten million) to 50,000,000 (fifty million) CFA francs or one of these two penalties only.

(2) The penalties provided for in paragraph 1 above are doubled if this results in either the deletion or modification of data contained in the information system, or an alteration of its operation.

Article 69.- Anyone who accesses without right, and in violation of security measures, all or part of an electronic communications network, an information system or terminal equipment, in order to obtain information or data, in relation to an information system connected to another information system, shall be punished by imprisonment of five (05) to ten (10) years and a fine of 10,000,000 (ten million) to 100,000,000 (one hundred million) CFA francs or one of these two penalties only.

Article 70.- Anyone who causes, by saturation, an attack on an electronic communications network resource or an information system with the aim of bringing it down by preventing the expected services from being provided shall be punished with a fine of 1,000,000 (one million) to 5,000,000 (five million) CFA francs.

Article 71.- Anyone who enters data into an information system or an electronic communications network without authority with a view to deleting or modifying the data contained therein shall be punished with imprisonment of two (02) to five (05) years and a fine of 1,000,000 (one million) to 25,000,000 (twenty-five million) CFA francs.

Article 72.- Anyone who, in any way whatsoever, without authority, introduces, alters, erases or deletes electronic data in such a way as to cause financial loss to another person in order to obtain economic benefit shall be punished by the penalties provided for in Article 66 above.

Article 73.- (1) Is punishable by imprisonment of two (02) to ten (10) years and a fine of 25,000,000 (twenty five million) to 50,000,000 (fifty million)
F CFA, or one of these two penalties only, anyone who, by means of an information system or in a counterfeit communications network, falsifies a payment, credit or withdrawal card or knowingly uses or attempts to use a counterfeit or falsified payment, credit or withdrawal card.

(2) Anyone who knowingly agrees to receive payment by electronic means using a counterfeit or falsified payment, credit or withdrawal card shall be punished by the penalties provided for in paragraph 1 above.

Article 74.- (1) Whoever, by any means whatsoever, invades the privacy of another person's private life by fixing, recording or transmitting, without the consent of the author, electronic data of a private or confidential nature shall be punished with imprisonment of one (01) to two (02) years and a fine of 1,000,000 (one million) to 5,000,000 (five million) CFA francs.

(2) Persons who, without authority, intercept personal data during their transmission from one information system to another shall be liable to the penalties provided for in paragraph 1 above;

(3) Anyone who processes or causes to be processed, even through negligence, personal data in violation of the formalities prior to their implementation shall be punished with imprisonment of one (01) to three (03) years and a fine of 1,000,000 (one million) to 5,000,000 (five million) CFA francs or one of these two penalties only.

(4) The act of collecting by illicit means, personal data of a person with a view to infringing their privacy and reputation, shall be punished by imprisonment of six (06) months to two (02) years and a fine of 1,000,000 (one million) to 5,000,000 (five million) CFA francs or one of these two penalties only.

(5) The penalties provided for in paragraph 4 above are doubled against anyone who puts, causes to be put online, keeps or causes to be kept in computer memory, without the express consent of the person concerned, personal data which, directly or indirectly, reveal their tribal origins, their political or religious opinions, their trade union membership or

his morals.

(6) The penalties provided for in paragraph 5 above apply to persons who misuse information, in particular, when recording, classifying or transmitting it.

(7) Anyone who keeps information in a nominative or encrypted form beyond the legal duration indicated in the request for advice or the declaration prior to the implementation of automated processing shall be punished with imprisonment of six (06) months to two (02) years and a fine of 5,000,000 (five million) to 50,000,000 (fifty million) CFA francs, or one of these two penalties only.

(8) The penalties provided for in paragraph 7 above shall be imposed for the disclosure personal data that undermines the victim's reputation.

Article 75.- (1) Anyone who records and distributes for profit, by means of electronic communications or an information system without the consent of the person concerned, images that infringe on bodily integrity shall be punished with imprisonment of two (02) to five (05) years and a fine of 1,000,000 (one million) to 5,000,000 (five million) CFA francs or one of these two penalties only.

(2) This article does not apply when the recording and broadcasting result from the normal exercise of a profession whose purpose is to inform the public or are carried out in order to serve as evidence in court in accordance with the provisions of the Code of Criminal Procedure.

Article 76.- Anyone who creates, transports or distributes, by means of electronic communications or an information system, a message of a child pornographic nature, or of a nature likely to seriously harm the dignity of a child, shall be punished by imprisonment of five (05) to ten (10) years and a fine of 5,000,000 (five million) to 10,000,000 (ten million) CFA francs or one of these two penalties only.

Article 77.- (1) Anyone who, by means of electronic communications or an information system, commits an insult against a race or a religion shall be punished with imprisonment of two (02) to five (05) years and a fine of 2,000,000 (two million) to 5,000,000 (five million) CFA francs or one of these two penalties only.

(2) The penalties provided for in paragraph 1 above are doubled when the offence is committed with the aim of arousing hatred or contempt among citizens.

Article 78.- (1) Anyone who publishes or disseminates news by means of electronic communications or an information system without being able to provide proof of its veracity or to justify that he had good reason to believe in the truth of said news shall be punished with imprisonment of six (06) months to two (02) years and a fine of 5,000,000 (five million) to 10,000,000 (ten million) CFA francs or one of these two penalties only.

(2) The penalties provided for in paragraph 1 above are doubled when the offense is committed with the aim of disturbing the public peace.

Article 79.- The penalties for private outrage against public decency provided for in Article 295 of the Penal Code are imprisonment of five (05) to ten (10) years and a fine of 5,000,000 (five million) to 10,000,000 (ten million) CFA francs or one of these two penalties only, when the victim has been put in contact with the perpetrator of the said acts, through the use of electronic communications or information systems.

Article 80.- (1) Anyone who distributes, fixes, records or transmits, for a fee or free of charge, an image showing acts of pedophilia on a minor by means of electronic communications or an information system shall be punished with imprisonment of three (03) to six (06) years and a fine of 5,000,000 (five million) to 10,000,000 (ten million) CFA francs or one of these two penalties only.

(2) Anyone who offers, makes available or distributes, imports or exports, by any electronic means whatsoever, an image or representation of a paedophile nature shall be punished with the same penalties provided for in paragraph 1 above.

(3) Anyone who possesses in an electronic communications network or in an information system, an image or representation of a pedophile nature, shall be punished by imprisonment of one (01) to five (05) years and a fine of 5,000,000 (five million) to 10,000,000 (ten million) CFA francs or one of these two penalties only.

(4) The penalties provided for in paragraph 3 above are doubled when an electronic communications network has been used to disseminate the image or representation of the minor to the public.

(5) The provisions of this article also apply to pornographic images depicting minors.

Article 81.- (1) The following acts shall be punishable by the penalties provided for in Article 82 below, when committed using an electronic communications network or an information system:

- the offering, production, making available of child pornography for the purpose of its distribution;
- procuring or procuring child pornography for others through an information system;
- the fact that adults make sexual propositions to minors under fifteen (15) years of age or a person presenting themselves as such;
- the dissemination or transmission of child pornography through an information system.

(2) Any act that is considered child pornography visually presenting:

- a minor engaging in sexually explicit conduct;
- a person who appears to be a minor engaging in a sexually explicit behavior;
- realistic images showing a minor engaging in a sexually explicit behavior.

Article 82.- Anyone who commits or attempts to commit by means of electronic communications an outrage against the public decency of a minor under the age of fifteen (15) shall be punished with double the penalties provided for in Article 79 of this law. years.

Article 83.- (1) Anyone who makes sexual propositions to a person of the same sex by means of electronic communications shall be punished with imprisonment of one (01) to two (02) years and a fine of 500,000 (five hundred thousand) to 1,000,000 (one million) CFA francs or one of these two penalties only.

(2) The penalties provided for in paragraph 1 above are doubled when The proposals were followed by sexual intercourse.

Article 84.- (1) Anyone who accesses, fraudulently becomes aware of, delays access to or deletes electronic communications addressed to others shall be punished by imprisonment of six months (06) to two (02) years and a fine of 500,000 to 1,000,000 CFA francs or one of these two penalties only.

(2) Any person who intercepts without authorization, diverts, uses or discloses electronic communications sent or received by electronic means or installs devices designed to carry out such interceptions shall be punished with the same penalties provided for in paragraph 1 above.

Article 85.- Anyone who, while carrying out a public service mission, acting in the exercise or on the occasion of the exercise of his functions, diverts or facilitates the diversion, deletion or access to electronic communications or the revelation of the content of these communications shall be punished by the penalties provided for in Article 84 above.

Article 86.- (1) Anyone who imports, holds, offers, transfers, sells or makes available, in any form whatsoever, a computer program, a password, an access code or any similar computer data designed and/or specially adapted to allow access to all or part of an electronic communications network or an information system shall be punished by the penalties provided for in Article 71 above.

(2) Anyone who causes a serious disruption or interruption of an electronic communications network or an information system with the intention of undermining the integrity of the data shall also be punished with the same penalties provided for in paragraph 1 above.

Article 87.- The perpetrators of one of the offences provided for in Article 86 above also incur the following additional penalties:

- confiscation in accordance with the terms provided for in Article 35 of the Code Criminal, of any object used or intended to commit the offense or considered to be the product thereof, with the exception of objects capable of restitution;

- the prohibition under the conditions provided for by article 36 of the Code Criminal, for a period of at least five (05) years, of exercising a public function or a socio-professional activity, when the acts were committed in the exercise or on the occasion of the exercise of functions;

- closure, under the conditions provided for in article 34 of the Code Penalty for a period of at least five (05) years, of the establishments or one or more of the establishments of the company used to commit the incriminated acts;

- exclusion, for a period of at least five (05) years, from markets public.

Article 88.- 1) Anyone who, having knowledge of the secret decryption agreement, of a means of cryptography likely to have been used to prepare, facilitate or commit a crime or an offense, refuses to hand over the said agreement to the judicial authorities or to implement it, upon the requisition of these authorities, shall be punished with imprisonment of (01) to five (05) years and a fine of 100,000 (one hundred thousand) to 1,000,000 (one million) CFA francs or one of these two penalties only.

(2) If the refusal is made when the delivery or implementation of the agreement would have made it possible to avoid the commission of a crime or an offense or to limit its effects, the penalties provided for in paragraph 1 above are increased from three (03) to five (05) years of imprisonment and the fine from 1,000,000 (one million) to 5,000,000 (five million) CFA francs.

Article 89.- Suspension of sentence may not be granted for the offences provided for in this law.

TITLE IV
INTERNATIONAL COOPERATION AND JUDICIAL ASSISTANCE

CHAPTER I
INTERNATIONAL COOPERATION

Article 90.- (1) In the exercise of their activities, Cameroonian certification authorities may, under the control of the Agency, establish agreements with foreign certification authorities.

(2) The procedures for establishing the agreements provided for in paragraph 1 above are determined by regulation.

CHAPTER II
INTERNATIONAL MUTUAL LEGAL ASSISTANCE

Article 91.- (1) Unless an international convention to which Cameroon is a party provides otherwise, requests for mutual assistance from Cameroonian judicial authorities to foreign judicial authorities shall be transmitted through the Ministry of Foreign Affairs. The execution documents shall be returned to the authorities of the requesting State by the same means.

(2) Requests for mutual assistance from foreign judicial authorities to Cameroonian judicial authorities must be submitted through diplomatic channels by the foreign Government concerned. The execution documents are returned to the authorities of the requesting State through the same channels.

(3) In cases of emergency, requests for mutual assistance requested by Cameroonian or foreign authorities may be transmitted directly to the authorities of the requested State for execution. The execution documents are returned to the competent authorities of the requesting State in accordance with the same procedures.

(4) Subject to international conventions, requests for mutual assistance from foreign judicial authorities to Cameroonian judicial authorities must be notified by the foreign government concerned. This notice shall be transmitted to the competent judicial authorities through diplomatic channels.

(5) In cases of emergency, requests for mutual assistance from foreign judicial authorities shall be forwarded to the Public Prosecutor or the territorially competent Investigating Judge.

(6) If the Public Prosecutor receives directly from a foreign authority a request for mutual assistance which can only be executed by the Examining Magistrate, he shall transmit it to the latter for execution or refer the matter to the Attorney General in the case provided for in Article 94 of this law.

(7) Before proceeding with the execution of a request for mutual assistance which has been directly referred to him, the Examining Magistrate shall immediately communicate it to the Public Prosecutor for advice.

Article 92.- (1) Requests for mutual assistance from foreign judicial authorities shall be executed by the Public Prosecutor or by the officers or agents of the Judicial Police requested for this purpose by this magistrate.

(2) They are carried out by the Examining Magistrate or by Judicial Police officers acting on a letter of request from this magistrate when they require certain procedural acts which can only be ordered or carried out during a preliminary investigation.

Article 93.- (1) Requests for mutual assistance from foreign judicial authorities shall be executed in accordance with the procedural rules provided for in the Code of Criminal Procedure.

(2) However, if the request for mutual assistance so specifies, it shall be executed in accordance with the procedural rules expressly indicated by the competent authorities of the requesting State, without these rules reducing the rights of the parties or the procedural guarantees provided for by the Code of Criminal Procedure.

(3) Where the request for mutual assistance cannot be executed in accordance with the requirements of the requesting State, the competent Cameroonian authorities shall inform the authorities of the requesting State without delay and indicate under what conditions the request could be executed.

(4) The competent Cameroonian authorities and those of the requesting State may subsequently agree on the action to be taken on the request, where appropriate, making it subject to compliance with the said conditions.

(5) The irregularity of the transmission of the request for mutual assistance cannot constitute a cause for nullity of the acts carried out in execution of this request.

Article 94.- (1) If the execution of a request for mutual assistance from a foreign judicial authority is likely to undermine public order or the essential interests of the Nation, the Public Prosecutor, having been notified of this request, shall transmit it to the Attorney General, who shall refer it to the Minister responsible for Justice and, where appropriate, shall notify the Public Prosecutor of this transmission.

(2) If the Minister responsible for Justice is notified, he shall inform the requesting authority, where appropriate, that his request cannot be granted, in whole or in part. This information shall be notified to the judicial authority concerned and shall prevent the execution of the request for mutual assistance or the return of the enforcement documents.

TITLE V
TRANSITIONAL AND FINAL PROVISIONS

Article 95.- Implementing texts establish, as necessary, the methods of application of this law.

Article 96.- Authorisations and declarations for the supply, import and export of means of cryptography issued by the competent authorities remain valid until the expiry of the period provided for by them.

Article 97.- This law shall be registered and published following the emergency procedure, then inserted in the Official Journal in French and English./-

YAOUNDE, THE

THE PRESIDENT OF THE REPUBLIC,

PAUL BIYA