REPUBLIQUE DU CAMEROUN

Paix – Travail – Patrie

REPUBLIC OF CAMEROON

Peace – Work – Fatherland

LAW N° 2010/012 OF 21 DECEMBER 2010 RELATING TO CYBERSECURITY AND CYBERCRIMINALITY IN CAMEROON

The National Assembly deliberated and adopted,
The President of the Republic hereby enacts the law set out below:

PART I
GENERAL PROVISIONS

Section 1 : This law governs the security framework of electronic communication networks and information systems, defines and punishes offences related to the use of information and communication technologies in Cameroon.

Accordingly, it seeks notably to:

- build trust in electronic communication networks and information systems;
- establish the legal regime of digital evidence, security, cryptography and electronic certification activities;
- protect basic human rights, in particular the right to human dignity, honour and respect of privacy, as well as the legitimate interests of corporate bodies.

Section 2. This law shall not cover the specific applications used in national defense and security.

Section 3. The electronic communication networks targeted by this law shall include: satellite, ground and electronic networks when they are used to route electronic communications and audio-visual communication broadcast or distribution networks.

Section 4. Within the meaning of this law and its implementing instruments, the following definitions shall be accepted:

(1) **Illegal access** : unauthorized intentional access to all or part of an electronic communication network, an information system or terminal equipment;

(2) **Administration in charge of telecommunications**: ministry or minister, as the case may be, invested with general powers over telecommunications and information and communication technologies by the Government;

(3) **Algorithm**: series of basic mathematical operations to be applied to data to achieve a desired result;

(4) **Asymmetric algorithm**: cipher algorithm using a public key to cipher and a private key (different) to decipher messages;

(5) **Symmetric algorithm**: cipher algorithm using the same key to cipher and decipher messages;

(6) **Active attack**: action modifying or altering the resources targeted by the attack (violation of the integrity and confidentiality of data);

(7) **Passive attack**: action that does not alter its target (eavesdropping, invasion of privacy);

(8) **Integrity violation**: action carried out intentionally to substantially disrupt or disable an information system, electronic communication network or terminal equipment by inputting, transmitting, damaging, deleting, deteriorating, altering suppressing or making data inaccessible;

(9) **Security audit**: systematic examination of components and security actors, policies, actions, procedures and resources used by an organization to protect its environment, conduct compliance tests controls to assess the adequacy of (organizational, technical, human and financial) resources allocated for risks, optimization, efficiency and performance;

(10) **Authentication**: safety criteria defined using a specific process to verify the identity of a person or entity and ensure that the identification given corresponds to the identity of the person initially registered;

(11) **Certification Authority**: trusted authority responsible for the creation and assignment of public and private keys and electronic certificates;

(12) **Root Certification Authority**: structure put in place in charge of the mission of accreditation of certification authorities, validating certification policy of certification authorities accredited, validating and signing certification authorities accredited certificates,

(13) **Digital certificate**: electronic record secured by the electronic signature of the person who issued it after ensuring that it certifies the authenticity of its contents;

(14) **Qualified electronic certificate**: digital certificate issued by a licensed Certification Authority;

(15) **Electronic certification**: issuance of electronic certificates;

(16) **Cipher**: the transformation of information using a secret key to make it illegible to anyone except those possessing special knowledge of the key;

(17) **Key**: in a cipher system, it corresponds to a mathematical value, a word, or a phrase which enables the ciphering or deciphering of a message with the help of the encryption algorithm;

(18) **Private key**: key used in asymmetric cipher mechanism (or public key cipher) which belongs to an entity and kept secret;

(19) **Public key**: used to cipher a message in an asymmetric system distributed freely;

(20) **Secret key**: key known to the sender and recipient used to cipher and decrypt messages using the symmetric cipher mechanism;

(21) **Source code**: all technical specifications, with no restrictions on access or implementation of a software or communication protocol, interconnection, interchange, or data format;

(22) **Audiovisual communication**: public communication by television and radio broadcasting services;

(23) **Electronic communication**: electromagnetic emission, transmission or reception of signs, signals, writings, images or sounds;

(24) **Confidentiality**: maintenance of the confidentiality of information and transactions to prevent unauthorized disclosure of information to non-recipients enabling the reading, listening, intentional or accidental, illegal copying during storage, processing or transfer;

(25) **Content:** all information relating to data belonging to individuals or legal entities, transmitted or received through electronic communication networks and information systems;

(26) **Illegal content**: content that infringes on human dignity, privacy, honour or national security;

(27) **Electronic mail**: message in the form of text, voice, sound or image transmitted through a public communication network, stored in a network server or the recipient's terminal equipment until he retrieves it;

(28) **Encryption**: use of codes or signals to convert information to be transmitted in the form of signals that are not understood by others;

(29) **Cryptanalysis**: all resources used to analyze initially encrypted information to be decrypted;

(30) **Encrypted text**: encrypted or encoded message;

(31) **Cryptography**: use of mathematical algorithm to encrypt information in an attempt to make it unintelligible to those who are not authorized to access it;

(32) **Cybercriminality**: infraction of the law carried out through cyberspace using means other than those habitually used to commit conventional crimes;

(33) **Cybersecurity**: technical, organizational, legal, financial, human, procedural measures for prevention and deterrence and other actions carried out to attain set security objectives through electronic communication networks and information systems, and to protect privacy;

(34) **Certification practice statement**: practices (organization, operational procedures, technical and human resources) that the competent certification authority applies within the framework of the provision of this service in accordance with the certification of a policy or policies it undertook to comply with;

(35) **Decryption**: reverse of encryption;

(36) **Denial of service**: attack by saturation of a resource of the information system or electronic communication network to make it collapse and unable to provide expected services;

(37) **Distributed Denial of Service**: simultaneous attack of the resources of an information system or electronic communication network in order to saturate and amplify the effects of interference;

(38) **Availability**: security criterion of resources of electronic communication networks, information systems and terminal equipment being accessible and usable as required (time factor);

(39) **Device for electronic signature creation**: equipment and/or .private encryption software certified by a competent authority, configured to create an electronic signature;

(40) **Device for electronic signature verification**: equipment and/or public encryption software certified by a competent authority used by a certifying authority to verify electronic signatures;

(41) **Data**: representation of facts, information or concepts in a form suitable for processing by terminal equipment, including a program allowing it to perform a function;

(42) **Connection data**: 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 or type of underlying service;

(44) **Terminal equipment**: equipment, installation or facilities to be connected to the endpoint of an information system which broadcasts, receives, processes and stores information data;

(45) **Reliability**: ability of an information system or electronic communication's network to operate without any incident for a very long time;

(46) **Provider of electronic communication services** : natural person or corporate body providing services consisting entirely or mainly in the provision of electronic communications;

(47) **Impact severity**: assessment of the gravity of an incident, weighted by its frequency of occurrence;

(48) **Data integrity**: safety criterion defining the status of an electronic communication's network, an information system or terminal equipment that remains intact and helps ensure that resources have not been altered (modified or destroyed) intentionally and accidentally to ensure their accuracy, reliability and durability;

(49) **Unlawful interception**: illegal or unauthorized access to the data of an electronic communication's network, an information system or a terminal equipment;

(50) **Lawful interception**: authorized access to the data of an electronic communication's network, an information system or terminal equipment without right or authorization;

(51) **Intentional intrusion**: intentional and unauthorized access to an electronic communication's network or an information system with the intent of causing harm or deriving economic, financial ,industrial , or security benefit or sovereignty;

(52) **Intrusion by intellectual challenge**: intentional access without right to an electronic communication's network or an information system with the intent of taking up an intellectual challenge that can help improve the performance of the organization's security system;

(53) **Deceptive software**: software that performs operations on a user's terminal equipment without initially informing him of the exact nature of the operations to be performed on his terminal equipment by the software or without asking his approval for the software to perform the operations;

(54) **Spyware**: specific deceptive software that collects personal information (most visited websites, passwords, etc.) from a user's electronic communication's network;

(55) **Potentially unwanted software**: software having the features of a deceptive software or spyware;

(56) **Plain text**: version .of a message that is intelligible to and understandable by all;

(57) **Cryptographic means**: equipment or software designed or modified used in transforming data, be it information or signals, using secret codes or to perform an inverse operation with or without a secret code to guarantee the safe storage or transmission of data and ensure the confidentiality and control of their integrity;

(58) **Non-repudiation**: security criterion that ensures the availability of evidence that can be used to prove the traceability of an electronic communication that has taken place;

(59) **Certificate policy**: set of rules that define standards to be respected by Certification Authorities when providing their services, indicating the applicability of a certificate to a particular community and/or class of application with common security requirements;

(60) **Security policy**: security benchmark established by an organization which reflects its security strategy and specifies the means to achieve it;

(61) **Provision of cryptographic service**: operation aimed at implementing cryptographic solutions on behalf of others;

(62) **Electronic communication's network**: active or inactive transmission systems and , where applicable, switching and routing equipment and other resources that enable signal routing by wire, radio, optical means or other electromagnetic means, including satellite, terrestrial networks, fixed (circuits or packets switching, including the Internet) and mobile networks, systems using electrical network, provided they are used to transmit signals, networks used for radio and television and cable television networks, irrespective of the type of information transmitted;

(63) **Telecommunication network**: installation or group of installations used in the transmission and routing of telecommunications signals, or exchange of command and management information associated with these signals between network points;

(64) **Security**: situation in which someone or something is not exposed to any danger. Mechanism to prevent any havoc or their attendant effect**s;**

(65) **Certification service**: service provided by a Certification Authority;

(66) **Electronic communication's service**: service consisting wholly or mainly in the provision of electronic communications, except the content of audiovisual communication services;

(67) **Representative**: individual acting on his own behalf or on behalf of the person or entity he represents, which involves a device for creating an electronic signature;

(68) **Electronic signature**: signature obtained by an asymmetric encryption algorithm to authenticate the sender of a message and verify its integrity;

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

(70) **Open standard**: communication, interconnection or exchange and interoperable data format protocol whose technical specifications and access are public and have no restriction or implementation;

(71) **Detection system**: system that helps detect incidents that could lead to security policy violation and help diagnose potential intrusions;

(72) **Information system**: devices or group of interconnected or related devices performing, by itself or by one or many of its components, automatic data processing, in line with a program;

(73) **Vulnerability**: security breach resulting either intentionally or accidentally by a violation of security policy in the architecture of an electronic communication's network, in designing an information system.

Section 5. The terms and expressions not defined under this law shall maintain their definitions or meanings as provided for in international legal instruments to which Cameroon adheres, notably the Constitution and the Convention of the International Telecommunications Union, the Radiocommunications' Regulation and the International Telecommunications' Regulation.

PART 11

CHAPTER 1
ELECTRONIC SECURITY AND GENERAL SECURITY CYBERSECURITY

Section 6. The Administration in charge of Telecommunications shall formulate and implement the electronic communication's security policy by taking into account technological developments and Government priorities in this domain.
Accordingly, it shall:

- promote the security of electronic communication networks and information systems and monitor the evolution of issues related to security and certification activities;
- coordinate activities that contribute to the security and protection of electronic communication networks and information systems at national level;
- ensure the setting up of an electronic communication's security framework; draw up the list of Certification Authorities; represent Cameroon in international bodies in charge of activities related to the security and protection of electronic communication networks and information systems.

CHAPTER 11
REGULATION AND MONITORING OF ELECTRONIC SECURITY ACTIVITIES

Section 7. (1) The National Agency for Information and Communication Technologies, hereinafter referred to as the Agency, instituted by the Law governing electronic communications in Cameroon, shall be responsible for the regulation of electronic security activities in collaboration with the Telecommunications Regulatory Board.

(2) The Agency referred to in subsection 1 above shall be responsible for the regulation , control and monitoring of activities related to the security of electronic communication networks, information systems, and electronic certification on behalf of the State.

Accordingly, its missions shall be to:

- examine applications for accreditation and prepare the specifications of Certification Authorities and submit them to the Minister in charge of telecommunications for signature;

- control the compliance of electronic signatures issued;

- participate in the development of the national policy on the security of electronic communication networks and certification;

- give an advisory opinion on instruments that fall under its area of competence;

- control activities aimed at ensuring the security of electronic communication networks, certification and information systems;

- examine applications for the certification of cryptographic means and issue certificates of homologation for security equipment;

- prepare agreements of mutual. recognition with foreign parties and submit them to the Minister in charge of Telecommunication for signature;

- monitor technological developments and issue warnings and recommendations regarding the security of electronic communication networks and certification ;

- participate in research, training and studies related to the security of electronic communication networks, certification and information systems;

- ensure the regularity and efficiency of security audits of information systems in accordance with established standards, public bodies and Certification Authorities

- monitor, detect and provide information on computer-related risks and cybercriminal activities;

- carry out any other mission of general interest assigned to it by the supervisory authority.

(3) A decree of the Prime Minister shall determine the modalities of implementation of subsection 1 above.

Section 8. (1) The Agency shall be the Root Certification Authority.
(2) The Agency shall be the Certification Authority of the Public Administration.

Section 9. (1) The Certification Authorities, security auditors, editors of security programs and other authorized security services are subject to the payment of a 1.5 % annual contribution of their untaxed turnover value intended to a fund named "Special Fund for Security Activities," intended to finance research, development, training and studies in respect of cybersecurity.

(2) The resources referred to in Subsection 1 above shall be collected by the Agency and deposited in an account opened at the Central Bank.

(3) A Committee is hereby created to be in charge of the validation of priority projects for research, development, training and studies in the domain of cybersecurity.
The conditions and terms for the functioning of the Committee shall be defined by regulation .

(4) The Minister in charge of Telecommunications shall be the authorizing officer for expenses made under the fund referred to in subsection 1 above.

(5) The conditions and terms of collection and management of this contribution shall be defined by regulation.

CHAPTER III
LEGAL REGIME OF CERTIFICATION ACTIVITIES

Section 10. Electronic certification activities shall be subject to prior approval. It shall be carried out by Certification Authorities.

Section 11. The following activities may be subject to authorization:

- the setting up and exploitation of infrastructure to issue, preserve and deliver qualified

electronic certificates;

- the provision of public keys to all public users;

- the provision of security auditing, security programs editing, and other authorized security services to the public.

Section 12. The conditions and terms for granting the authorization referred to in Section 10 above shall be laid down by regulation.

CHAPTER IV
SECURITY ACTIVITIES

Section 13. (1) Electronic communication networks and information systems of operators, certification authorities and electronic communication service providers shall be subject to an obligatory security audit.

2) The conditions and terms for the conduct of the security audits provided for in Sub-Section 1 above shall be laid down by regulation .

Section 14. The staff of the Agency and experts recruited to carry out audit operations shall be required to maintain professional secrecy.

CHAPTER V
ELECTRONIC CERTIFICATION

Section 15. (1) Qualified electronic certificates shall be valid only for the objects for which they were issued.

(2) Devices used to design and verify qualified certificates shall, from the technological standpoint, be neutral, standardized, certified and interoperable.

Section 16. (1) Certification Authorities shall be responsible for prejudice caused to .people who relied on the certificates they presented as qualified in the case where:

- the information contained in the certificate on the date of its issuance was inaccurate;
- the data prescribed such that certificate could be considered as qualified was incomplete
- the issuance of the qualified certificate did not give rise to the verification that the signatory holds the private convention corresponding to the public convention of the certificate;
- Certification Authorities and certification service providers, as the case may be, have not registered the repeal of the qualified certificate and placed this information at the disposal of third parties.

(2) Certification Authorities shall not be responsible for the prejudice caused by the use of the qualified certificate that exceeds the limits fixed for its use or the value of transactions for which it can be used, provided that such limits appear in the qualified certificate and are accessible to users.

(3) Certification Authorities must justify adequate financial guarantee, allocated particularly for the payment of sums they may *owe* people who relied logically on the qualified certificates they issue, or an insurance that guarantees the pecuniary consequences of their civil professional responsibility.

CHAPTER VI
ELECTRONIC SIGNATURE

Section 17. The advanced electronic signature shall have the same legal value as that handwritten signature and produce the same effects as the latter.

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

- the data related to signature creation shall be exclusively linked to the signatory and be under his exclusive control;
- each modification shall be easily detectable;
- it shall be created using a protected device whose technical characteristics shall be defined by an instrument of the Minister in charge of telecommunications;
- the certificate used to generate signatures shall be a qualified certificate. An instrument of the Ministry in charge of telecommunications shall determine the criteria of the qualification of certificates.

CHAPTER VII
ELECTRONIC CERTIFICATES AND SIGNATURES ISSUED BY CERTIFICATION AUTHORITIES

Section 19. The certification authority that validated an electronic certificate may not retract.

Section 20. (1) An electronic certificate issued outside the national territory shall produce the same legal effects as a qualified certificate issued in Cameroon provided that there is a decision recognizing the issuing authority by the Minister in charge of telecommunications.

(2) The interoperability of qualified electronic certificates shall be regulated by an instrument of the Minister in charge of telecommunications.

CHAPTER VIII
ELECTRONIC DOCUMENT

Section 21. Any person wishing to affix his electronic signature to a document can create the signature using a reliable device whose technical characteristics shall be determined by instrument of the Minister in charge of Telecommunications.

Section 22. Any person using an electronic signature device must:

- take minimum precautions fixed by the instrument referred to in Section 21 above to avoid any illegal use of the encoding elements or personal equipment related to its signature;
- inform the Certification Authority about any illegitimate use of his signature;
- ensure the authenticity of all the data he declared to the electronic certification service

provider and to any person he **requested to trust his signature.**

Section 23. In the event of failure to honor the commitments under Section 22 above, the holder of the signature shall be responsible for the injury caused to others.

CHAPTER IX
PROTECTION OF ELECTRONIC COMMUNICATION NETWORKS, INFORMATION SYSTEMS AND PERSONAL PRIVACY

1- PROTECTION OF ELECTRONIC COMMUNICATION NETWORKS

Section 24. Electronic communication networks operators and electronic communication service providers must take all the necessary technical and administrative measures to guarantee the security of the services provided. To that end, they shall be bound to inform users about:

- the risks of using their networks;
- the specific risks of security violation , notably the denial of services distributed, abnormal rerouting, traffic points, traffic and unusual ports, passive and active listening, intrusion and any other risk;
- the existence of techniques to ensure the security of their communications.

Section 25. (1) Network operators and electronic communication service providers shall be bound to conserve traffic connection data for a period of 10 (ten) years.

(2) Network operators and electronic communication service providers shall set up mechanisms for monitoring the traffic data of their networks. Such data may be accessible in the course of judicial inquiries.

(3) Network operators and electronic communication service providers shall be liable where the use of the data referred to in Sub-section 2 above undermines the individual liberties of users.

II - PROTECTION OF INFORMATION SYSTEMS

Section 26. (1) Operators of information systems shall take every technical and administrative measure to ensure the security of services offered . To this end, they shall have standardized systems enabling them to at all times identify, assess, process or manage any risk relating to the security of the information systems of the services provided directly or indirectly.

(2) Operators of information systems shall set up technical mechanisms to avoid any hitches that may be prejudicial to the steady functioning of systems, their integrity, authentication, non repudiation by third party users, confidentiality of data and physical security.
(3) The mechanisms provided for in Subsection 2 above shall be subject to the approval and visa of the Agency.

(4) Information systems platforms shall be protected against any radiation or intrusion that may impair the integrity of data transmitted and any other external attack notably, through intrusions detection system.

Section 27. Corporate bodies whose activity is to provide access to information systems shall be bound to inform users of:

- the dangers associated with the use of unprotected information systems notably for private individuals;
- the need to install parental control devices;
- specific security violation risks notably, the generic family of viruses;
- the existence of permanent technical means to restrict access to certain services and propose to them at least one of such means notably, the use of the most recent operating systems, the use of anti-viruses against spywares, misleading viruses, the activation of personal firewalls, intrusion detection systems and activation of automatic updating.

Section 28. (1) Operators of information systems shall inform users of the prohibition to use electronic communication networks for the publishing of illicit content or any other act that IS likely to affect the security of networks or information systems.

(2) Such prohibition shall equally concern the designing of misleading viruses, spywares, potentially undesirable software or any other device leading to fraudulent practices.

Section 29. (1) Operators of information systems shall be bound to conserve the connection and traffic data of their information systems for a period of 10 (ten) years.

(2) Operators of information systems shall be bound to set up mechanisms for monitoring and controlling access to the data of their information systems. Such data may be accessible in the course of judicial inquiries.

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

Section 30: (1) Operators of information systems shall assess and revise their security systems and, where necessary, make the appropriate modifications to their security practices, measures and techniques according to technological change.

(2) Operators of information systems and users may cooperate mutually with a view to implementing the security practices, measures and techniques of their systems.

Section 31. (1) Electronic communication networks and information systems content providers shall be bound to ensure the availability of material, as well as the data stored in their installations.

(2) They shall be bound to set up filters in order to avoid any attacks that may be prejudicial to personal data and the privacy of users.

Section 32. (1) Electronic communication networks and information systems shall be subject to a regime of compulsory and periodic auditing of their security systems by the Agency.

(2) Security audit and severity scale rating shall be undertaken each year or as required by the prevailing circumstances.

(3) Audit reports shall be confidential and addressed to the Minister in charge of Telecommunications.

(4) An instrument of the Minister in charge of Telecommunications shall fix conditions for rating the severity scale.

III - OBLIGATIONS OF ACCESS, SERVICE AND CONTENT PROVIDERS

Section 33. Persons whose activity consists in providing access to electronic communication services shall inform their subscribers of the existence of technical means of restricting access to certain services of choosing them and propose to them at least one of such means.

Section 34. (1) The persons in charge, even gratuitously, of the storage of signals, written material, images, sound or messages of any nature supplied by the users of such services may be liable.

(2) However, the liability under sub-section 1 above shall not apply where:

- the said persons were not effectively aware of the illicit nature of the facts or circumstances characterizing them as such;
- once they became aware of the facts, acted promptly to withdraw such data or render them inaccessible.

Section 35. (1) The persons referred to in Sections 33 and 34 above shall be bound to preserve, for a period of 10 (ten) years, data enabling the identification of any person who contributed to the creation of the content of the services they provided.

(2) They shall provide the persons who edit electronic .communication services with the technical means enabling them to fulfil the identification conditions referred to in Sections 37 and 38 below.

(3) A judicial authority may request the providers referred to in Sections 33 and 34 above to communicate communication data referred to in Subsection 1 above.

Section 36. The competent court referred to shall rule, within a maximum time-limit of 30 (thirty) days, on all measures to prevent or stop any damage caused by the content of an electronic communication service.

Section 37. Persons engaged in editing electronic communication services shall inform the public of:

- their full name, domicile and telephone numbers and, where they are subject to trade registration, personal property loan formalities and their registration number, in case of corporate bodies;

- their company or corporate name and head offices, telephone numbers and, where they are corporate bodies subject to trade registration, personal property loan formalities, their registration number, share capital, head office addresses, in case of corporate bodies;

- the name of the publisher or co-publisher and, where necessary, that of the editor in chief;

- the name, company or corporate name, address and telephone number of the provider referred to in Sections 33 and 34 above.

Section 38. (1) Persons editing an electronic communication's service may place at the disposal of the public only the name, company or corporate name and the address of the provider.

(2) The persons referred to in Sections 33 and 34 above shall be bound to confidentiality.

Section 39. (1) Any person who is victim of defamation by means of an electronic communication's service shall have the right to reply and may request for correction.

(3) Conditions for the insertion of a rejoinder of reply shall be those provided for by the instruments in force.

Section 40. (1) Any person engaged in transmitting electronic communication networks content or providing access to an electronic communication's network may not be liable where they:

- requested the contentious transmission;
- select or modify the content transmitted.

(2) Any person whose activity, for the sole purpose of rendering its subsequent transmission more efficient, is the automatic, intermediary and temporary storage of content transmitted by a provider, may be criminally or civilly liable in respect of such content only in the case where they modify such content, do not comply with the required conditions of access and ordinary updating rules or where they impede the licit and normal use of the technology used to obtain data.

IV - PROTECTION OF PRIVACY

Section 41. Every individual shall have the right to the protection of their privacy. Judges may take any protective measures notably, sequestration or seizure to avoid or end the invasion of privacy.

Section 42. The confidentiality of information channelled through electronic communication and information systems networks, including traffic data, shall be ensured by operators of electronic communication and networks information systems.

Section 43. Content providers shall be responsible for data transmitted through their information system notably, if such content may entail infringement of human dignity, injury to character and invasion of privacy.

Section 44. (1) It shall be forbidden for any natural person or corporate body to listen, intercept and store communications and the traffic data related thereto, or to subject them to any other means of interception or monitoring without the consent of the users concerned, save where such person is so authorized legally.

(2) However, technical storage prior to transmission of any communication shall be authorized for electronic communications' networks and information systems operators, without prejudice to the principle of confidentiality.

Section 45. The recording of communications and traffic data related thereto in a professional setting with a view to providing digital evidence of an electronic communication shall be authorized.

Section 46. (1) Electronic communication networks and information systems content providers shall be bound to conserve such content and stored data in their installations for a period of the 10 (ten) years.

(2) Electronic communication networks and information systems content providers shall be bound to set up liters in order to contain any attacks that may be prejudicial to the personal data in privacy of users.

Section 47. The use of electronic communication networks and information systems for the purpose of storing information or accessing information stored in the terminal equipment of a natural person or corporate body shall be made only with their prior consent.

Section 48. (1) The sending of electronic messages for prospecting purposes by dissimilating the sender identity or without indicating the valid address to which the addressee may send a request aimed at blocking such information shall be prohibited.

(2) The sending of electronic mails by usurping the identity of another user shall be prohibited.

V -INTERCEPTION OF ELECTRONIC COMMUNICATION

Section 49. Notwithstanding the provisions of the Criminal Procedure Code, in case of crimes or offences provided for hereunder, criminal investigation officers may intercept record or transcribe any electronic communication.

Section 50. In the event of encoding, compressing or ciphering of data transmitted by electronic communication networks or electronic communication service providers, clear corresponding interceptions shall be provided to the services that requested them.

Section 51. The personnel of electronic communication network operators or electronic communication service providers shall be bound to secrecy for any requests they receive.

PART III
CYBERCRIMINALITY
CHAPTER 1
PROCEDURAL LAW PROVISIONS

Section 52. (1) In case of any cyberoffence, Criminal Investigation Officers with general jurisdiction and authorized officials of the Agency shall carry out investigations, in accordance with the provisions of the Criminal Procedure Code.

(2) Prior to assuming duty, authorized officials of the Agency shall take an oath before the competent Court of First Instance as follows : "I swear to perform my duties loyally and to always abide by the responsibilities bestowed on me, to keep secret information I am aware of on the occasion of or in the discharge of my duties".

(3) Criminal Investigation Officers and authorized officials of the Agency, may in the course of investigations, have access to means of transport, any professional premises, with the exception of private residences, with a view to seeking and recording offences, requesting the production of all professional documents and taking copies thereof and gathering any information and evidence, upon a summons or in situ.

Section 53. (1) Cybercriminal-related searches may concern data. Such data may be physical material or copies made in the presence of persons taking part in the search.

(2) When a copy of seized data is made, it may, for security reasons be destroyed on the instruction of the State Counsel.

(3) On the approval of State Counsel, only objects, documents and data used as evidence may be kept under seal.

(4) Persons present during searches may be requested to provide information on any seized objects, document and data.

Section 54. Searches and seizures shall be carried out in accordance with the provisions of the Criminal Procedure Code, taking into account the loss of validity of evidence.

Section 55. (1) When it appears that data seized or obtained in the course of an investigation or inquiry has been the subject of transformation, thus hindering clear access or is likely to impair the information it contains, the State Counsel, the Examining Judge or the Court may request any qualified natural person or corporate body to perform technical operations to obtain the clear version of the said data.

(2) When a cryptographic means has been employed, judicial authorities may request the secret conversion of the encrypted text.

Section 56. The request provided for in Section 50 above may be made to any expert. In such case, it shall conform with the provisions of the Criminal Procedure Code relating to the commissioning of an expert.

Section 57. (1) Cameroonian judicial authorities may set up a rogatory commission at, both the national and international level, any corporate body or natural person to search the elements of cybercrime offences of which at least one of the elements was committed on Cameroonian territory or which one of the offenders or accomplices resides on the said territory.

(2) Subject to rules of reciprocity between Cameroon and foreign countries with which it has concluded a judicial cooperation agreement, rogatory commissions shall be executed in accordance with the provisions of the Criminal Procedure Code.

Section 58. (1) Natural persons or corporate bodies that provide cryptographic services aimed

at performing a duty of confidentiality shall be bound to hand over to criminal investigation officers or authorized officials of the Agency, at their request, the agreements allowing the conversion of data transformed by means of the services that they deliver.

(2) Criminal investigation officers and authorized officials of the Agency may request the service providers referred to in Sub-section 1 above to implement these agreements of their own motion, except where they are unable to satisfy such requests.

Section 59. (1) For purposes of investigation or examination, the hearing or interrogation of a person and/or confrontation of several persons may be carried out on several locations on the national territory linked by electronic communication means that ensure the confidentiality of transmissions. A report shall be drawn up on the operations carried out in each location. Such operations may be subject to audiovisual and/or sound recording.

(2) According to the prevailing circumstances, their interpretation may be done by means of electronic communication in the course of a hearing, interrogation or confrontation.

(3) The provisions of this Section shall equally be applicable for the concurrent implementation, on a location on the national territory or on a location situated outside the national territory, of mutual assistance requests from foreign judicial officers or acts of mutual assistance performed outside the national territory, at the request of Cameroonian judicial authorities.

(4) Conditions for the implementation of this section shall be defined by regulation.

CHAPTER II
OFFENCES AND PENALITIES

Section 60. (1) When a Certification Authority is non-compliant, the . Agency may, after serving a warning on the structure for comment, prohibit the circulation of the means of cryptography concerned.

(2) The prohibition of circulation shall be applicable throughout the national territory. It equally entails, for the provider, the obligation to withdraw:

- the means of cryptography whose circulation among commercial publishers was prohibited;
- materials that constitute a means of cryptography and whose circulation was prohibited and that was acquired directly or through commercial publishers for a consideration.

(3) The means of cryptography concerned could be put back into circulation once the previous obligations are fulfilled and duly ascertained be the Agency.

Section 61 . (1) Agency personnel and experts of corporate bodies in charge of security audits who without any authorization, disclose confidential information they are privy to on the occasion of a security audit shall be punished with imprisonment for from three 03 (three) months to (three) 03 years and a fine of from 20,000 (twenty thousand) to 100,000 (one hundred) CFA francs.

(2) Refusal to comply with the summons of authorized officials shall be punished with imprisonment for from (three) 03 months to (four) 04 years.

(3) Whoever, by any means whatsoever, obstructs, gives incitement to resist or prevent the conduct of the investigation provided for in this section or refuses to provide information or documents related thereto shall be punished with imprisonment for from 01 (one) to 05 (five) years or a fine of from 100,000 (one hundred thousand) to 1,000,000 (one million) CFA francs or both of such fine and imprisonment.

Section 62. (1) Whoever presents the content or activity to the person referred to in Sections 33 and 34 above as illicit so as to cause the withdrawal or stop the publication thereof, knowing such information to be untrue, shall be punished with imprisonment for from 01 (one) to 05 (five) years and a fine of from 200,000 (two hundred thousand) to 2,000,000 (two million) CFA francs.

(2) The publisher, under pain of a fine of from 100,000 (one hundred thousand) to 2 000 000 (two million) CFA francs shall be bound to insert within 48 (forty-eight) hours of their reception , the response of any person designated in the electronic communication service.

Section 63. (1) The de jure or de facto manager of a corporate body exercising the activity defined in Sections 33 and 34 of this law who fails to conserve the information elements referred to in Sections 25 and 29 shall be punished with imprisonment for from 01 (one) to 05 (five) years and a fine of from 40 000 (forty thousand) to 4 000 000 (four million) CFA francs.

(2) The de jure or de facto manager of a corporate body exercising the activity defined in Sections 37 and 38 who fails to comply with the provisions of the said Sections shall be liable to the same sanctions.

Section 64. (1) Corporate bodies shall be criminally liable for offences committed on their account by their management structures.

(2) The criminal liability of corporate bodies shall not preclude that of natural persons who commit such offences or are accomplices.

(3) The penalties to be meted out on defaulting corporate bodies shall be fines of from 5 000 000 (five million) to 50 000 000 (fifty million) CFA francs.

(4) The penalties provided for in Subsection 3 above, not withstanding one of the following other penalties may equally be meted out on corporate bodies:

- dissolution in case of a crime or felony punishable with respect to natural persons with imprisonment of 03 (three) years and above and where the corporate body has departed from its declared object to aid and abet the incriminating acts;

- definitive prohibition or temporary prohibition for a period not less than 05 (five) years, from directly or indirectly carrying out one or more professional or corporate activities;

- temporary closure for a period of not less than 05 (five) years under the conditions laid

down in Section 34 of the Penal Code of the establishments or one or more establishments of the company that was used to commit the incriminating acts;

- barring from bidding for public contracts either definitively or for a period of not less than 05 (five) years;
- barring from offering for public issues either definitively or for a period of not less than 05 (five) years;

- prohibition for a period of not less than 05 (five) years from issuing cheques other than those to be used by the drawer to withdraw money from the drawer or certified checks or from using payment cards;

- seizure of the device used or intended to be used in committing the offence or the proceeds of the offence;

- publication or dissemination of the decision taken either through the print media or through any electronic means of communication to the public.

Section 65. (1) Whoever, without any right or authorization, proceeds by electronic means to intercept or not during transmission, intended for, whether or not within an electronic communication network, an information system or a terminal device shall be punished with imprisonment for from 05 (five) to 10 (ten) years or a fine of from 5.000.000 (five million) to 10.000.000 (ten million) CFA francs or both such fine and imprisonment.

(2) Any unauthorized access to all or part of an electronic communication network or an information system or a terminal device shall be liable to the same sanctions in accordance with Subsection 1 above.

(3) The penalties provided for in Subsection 1 above, shall be doubled where unauthorized access violates the integrity, confidentiality, availability of the electronic communication network or the information system.

(4) Whoever, without any right, allows access to an electronic communication network or an information system as an intellectual challenge shall be punished in accordance with Subsection 1 above.

Section 66. (1) Whoever causes disturbance or disruption of the functioning of an electronic communication network or a terminal device by introducing, transmitting, destroying, erasing, deteriorating, altering, deleting data or rendering data inaccessible shall be punished with imprisonment for from 02 (two) to 05 (five) years or a fine of from 1.000.000 (one million) to 2.000.000 (two million) CFA francs or both of such fine an imprisonment.

(2) Whoever uses the deceptive or undesirable software to carry out operations on a user's terminal device without first informing the latter of the true character of the operation which the said software is likely to damage shall be punishable with the same penalties.

(3) Whoever uses potentially undesirable software to collect, try to collect or facilitate any of such operations in order to access information of the operator or supplier of an electronic network or services and commit a crime shall be punishable in accordance with subsection 1 above.

Section 67. Causing serious disturbance or disruption of the functioning of an electronic communication network or terminal equipment by introducing, transmitting, changing, deleting or altering data shall constitute a breach of the integrity of an electronic communication network or an information system and shall be punishable in accordance with Section 66 above.

Section 68. (1) Whoever fraudulently gains access or remains in all or part of an electronic communication network or an information system by transmitting, destroying, causing serious disturbance or disruption to the functioning of the said system or network shall be punished with imprisonment for from 05 (five) to 10 (ten) years or a fine of from 10.000.000 (ten million) to 50.000.000 (fifty million) CFA francs or both of such fine and imprisonment.

(2) The same penalties provided for in subsection 1 above shall be doubled where such acts result in the deletion or change to the data contained in the information system or a change in its functioning.

Section 69. Whoever accesses all or part of an electronic communication network, an information system or terminal equipment without authorization and in violation of security measures in order to obtain information or data relating to an information system connected to another information system shall be punished with imprisonment for from 05 (five) to 10 (ten) years or a fine of from 10 000 000 (ten million) to 100,000,000 (one hundred thousand million) CFA francs or both of such fine and imprisonment.

Section 70. Whoever causes through saturation, the attack of an electronic communication network device or an information system with the intention to cause its collapse thus preventing it from rendering the expected services, shall be punished with a fine of from 1,000,000 (one million) to 5 000 000 (five million) CFA francs.

Section 71. Whoever without permission, introduces data into an information system or an electronic communication network in order to delete or change the data contained therein, shall be punished with imprisonment for from 02 (two) to 05 (five) years and a fine of from 1 000 000 (one million) to 25 000 000 (twenty five million) FCFA francs.

Section 72. Whoever without authorization and for financial gain, uses any means to introduce, alter, erase or delete electronic data such as to cause damage to someone else's property shall be punished with the penalties provided for in Section 66 above.

Section 73. (1) Whoever uses an information system or a counterfeit communication network to falsify payment, credit or cash withdrawal card or uses or attempts to use, in full knowledge of the facts, a counterfeit or falsified payment, credit or withdrawal card shall be punished with imprisonment for from 02 (two) to 10 (ten) years and a fine of from 25,000,000 (twenty five million) to 50 000 000 (fifty million) CFA francs or both of such fine and imprisonment.

(2) Whoever deliberately accepts to receive electronic communications payment using a forged or falsified payment, credit or cash withdrawal card shall be punished in accordance with Subsection 1 above.

Section 74. (1) Whoever uses any device to receive the privacy of another person by

attaching, recording or transmitting private or confidential electronic data without the consent of their authors shall be punished with imprisonment for from 01 (one) to 02 (two) years and a fine of from 1,000,000 (one million) to 5,000,000 (five million) CFA francs.

(2) Whoever, without authorization, intercepts personal data in the course of their transmission, from one information system to another, shall be punished in accordance with Subsection 1 above.

(3) Whoever, even through negligence processes or causes the processing of personal data in violation of the conditions precedent to their implementation shall be punished with imprisonment from 01 (one) to 03 (three) years and a fine of from 1,000,000 (one million) to 5,000,000 (five million) or both of such fine and imprisonment.

(4) Whoever uses illegal means to collect the personal data of another in order to invade his or her privacy and undermine his or herself esteem shall be punishable with imprisonment for from 06 (six) months to 02 (two) years or a fine of from 1 000,000 (one million) to 5,000,000 (five million) CFA francs or both of such fine and imprisonment.

5) The penalties provided for in Subsection 4 above shall be doubled where anyone posts online, stores or has someone else store in a computerized memory, without the express consent of the person concerned, personal data which directly or indirectly discloses his/her tribal origin, political opinions, religious beliefs, trade union membership or values.

(6) The penalties provided for in Subsection 5 above shall apply to persons found guilty of diverting information, in particular, during the recording, filing or transmission thereof.

7) Whoever keeps information in works or in figures beyond the legal time-limit specified in the application for a prior opinion or declaration for use of .data processing shall be punished with imprisonment for from 06 (six) months to 02 (two) years or a fine of from 5000000 (five million) to 50000000 (fifty million) CFA francs or both of such fine and imprisonment.

(8) Whoever discloses personal information that undermines the consideration due to the victim shall be punished with the penalties provided for in Subsection 7 above.

Section 75. (1) Whoever for financial gain, records or publishes images that undermine the bodily integrity of another person through electronic communications or an information system without the consent of the person concerned shall be punished with imprisonment for from 02 (two) years to 05 (five) years or a fine of from 1,000,000 (one million) to 5,000,000 (five million) CFA francs or both of such fine and imprisonment.

(2) This section shall not apply where such recording and publication fall under the normal exercise of profession aimed at informing the public on where they are carried out in order to be used as evidence in Court in accordance with the provisions of Criminal Procedure Code.

Section 76. Whoever uses electronic communications or an information system to design, carry or publish a child pornography message or a message likely to seriously injure the self-respect of a child shall be punished with imprisonment for from 5 (five) years to 10 (ten) years or a fine of from 5,000,000 (five million) to 10,000,000 CFA francs or both of such fine and imprisonment.

Section 77. (1) Whoever uses electronic communication or an information system to act in contempt of race or religion shall be punished with imprisonment for from 02 (two) years to 05 (five) years or a fine of from 2 000 000 (two million) to 5 000 000 (five million) CFA francs or both of such fine and imprisonment.

(2) The penalties provided for in Subsection 1 above shall be doubled where the offence is committed with the aim of stirring up hatred and contempt between citizens.

Section 78. (1) Whoever uses electronic communications or an information system to design, to publish or propagate a piece of information without being able to attest its veracity or prove that the said piece of information was true shall be punished with imprisonment for from 06 (six) months to 02 (two) years or a fine of from 5,000,000 (five million) to 10,000,000 (ten million) CFA francs or both of such fine and imprisonment.

(2) The penalties provided for in Subsection 1 above shall be doubled where the offence is committed with the aim of disturbing public peace.

Section 79. Penalties against private acts of indecency set forth in Section 295 of the Penal Code shall be punished with imprisonment for from 05 (five) years to 10 (ten) years or a fine of from 5,000,000 (five million) to 10,000,000 (ten million) CFA francs where the victim has been put in contact with the author of the said acts using electronic communication or an information system.

Section 80. (1) Whoever for consideration or free of charge, uses electronic communications or an information system to publish, attach, record or transmit an image showing acts of pedophilia or a minor shall be punished with imprisonment for from 01 (one) to 05 (five) years or a fine of from 5 000 000 (five million) to 10,000,000 (ten million) CFA francs or both of.such fine and imprisonment.

(2) Whoever uses electronic means whatsoever to offer, provide or publish, import or export an image or picture portraying pedophilia shall be punished with the penalties provided in Subsection 3 above.

(3) Whoever keeps an image or picture portraying pedophilia in an electronic communication network or an information system shall be punished with imprisonment for from 01 (one) to 05 (five) years or a fine of from 5,000,000 (five million) to 10,000,000 (ten million) CFA francs or both of such fine and imprisonment.

(4) The penalties provided for in Subsection 3 above shall be doubled where an electronic communication network is used to publish an image or picture of a minor.

(5) The provisions of this section shall equally apply to pornographic pictures showing minors.

Section 81. (1) The following offences shall be punishable with the penalties provided for in Section 82 below where they are committed using an electronic communication network or an information system:

- offering, producing, providing child pornography for publication;
- acquiring child pornography for oneself or for someone else using an information

system;
- where adult persons make sexual proposals to minors below 15 years old or to a person having the features of a minor;
- dissemination or transmission of child pornography using an information system.

(2) Child pornography shall be any act which visually presents:

- a minor involved in sexually explicit behavior;
- any person with the physical features of a minor involved in sexually explicit acts;
- real images of a minor involved in sexually explicit acts.

Section 82. The penalties provided for in Section 79 above shall be doubled for whoever uses electronic communication devices to commit or attempt to commit any act of indecency on a minor less than 15 (fifteen) years old.

Section 83. (1) Whoever uses electronic communication devices to make sexual proposal to a person of the same sex shall be punished with imprisonment for from 01 (one) to 02 (two) years or a fine of from 500,000 (five hundred thousand) to 1,000,000 (one million) CFA francs or both of such fine and imprisonment.

(2) The penalties provided for in subsection (1) above shall be doubled if sexual proposals are followed by sexual intercourse.

Section 84 (1) Whoever fraudulently becomes acquainted with, delays access to or deletes electronic messages addressed to another shall be punished with imprisonment for from 06 (six) months to 02 (two) years of a fine from 500,000 (five hundred thousand) to 1,000,000 (one million) CFA francs or both of such fine and imprisonment.

(2) The same penalties provided for in subsection 1 above shall apply against whoever, without authorization, intercepts, diverts, uses or divulges electronic messages sent or received by electronic means or proceeds to install equipment designed for such interceptions.

Section 85. The penalties provided for in section 84 above shall apply against whoever, being responsible for a public service mission and acting in the discharge or during the discharge of his/her duties, diverts or facilitates the diversion, deletion or access to electronic messages or reveals the content thereof.

Section 86. (1) The penalties provided for in section 71 above shall apply against whoever imports, keeps, offers, transfers, sells or provides, in any form whatsoever, a computer program, a password, an access code or any similar computer data designed and/or specially adapted to facilitate access to all or part of an electronic communication or an information system.

(2) Whoever causes serious disturbance or disruption on an electronic communication, or whoever uses electronic communication network or an information system with the intention of breaching the integrity of the data, shall be punishable with the penalties provided for in Subsection 1 above.

Section 87. Authors of the offences provided for in Section 86 above shall be punishable with the following additional penalties:

- seizure, in accordance with the conditions laid down in Section 35 of the Penal Code, of any object used or intended to be used to commit the offence or considered to be the proceed thereof, with the exception of objects likely to be restituted;
- prohibition, in accordance with the conditions laid down in Section 36 of the Penal Code, for a period of not less than 05 (five) years from the holding of a public office or carrying out a socio-professional activity where the offence was committed in the discharge or during the discharge of one's duties;
- closure, in accordance with the conditions laid down in \ Section 34 of the Penal Code, for a period of not less than 05 (five) years, of establishments or of one or more of the establishments of the company that was used to commit the offence;
- barring, for a period of not less than 05 (five) years, from **public contracts.**

Section 88. (1) Whoever, knowing about the secret decoding convention, a cryptographic means likely to have been used to prepare, facilitate or commit a crime or felony, refuses to hand over the said convention to judicial authorities or to use it upon request by such authorities shall be punished with imprisonment for from 01 (one) to 05 (five) years or a fine of from 1,000,000 (one million) to 5,000,000 (five million) CFA francs or both of such fine and imprisonment.

(2) Where such refusal occurs whereas the handing over or use of the convention could have helped prevent the commission of the crime or felony or limit the effects thereof, the penalties provided for in Subsection 1 above shall be increased to imprisonment for from 03 (three) to 05 (five) years and a fine of from 1 000000 (one million) to 5000000 (five million) CFA francs.

Section 89. There shall be no suspended sentence for the offences provided for in this law.

PART IV
INTERNATIONAL COOPERATION AND MUTUAL JUDICIAL ASSISTANCE

CHAPTER I
INTERNATIONAL COOPERATION

Section 90. (1) In the discharge of their duties, Cameroonian Certification Authorities may, under the control of the Agency, conclude conventions with foreign Certification Authorities.
(2) The conditions for concluding the conventions referred to in Subsection 1 above shall be laid down by regulation,

CHAPTER II
INTERNATIONAL AND MUTUAL JUDICIAL ASSISTANCE

Section 91 (1) Unless otherwise provided for by an international convention to which Cameroon is signatory, requests for judicial assistance from Cameroonian judicial officers to foreign judicial officers shall be sent through the Ministry in charge of External Relations. Enforcement documents shall be sent to the authorities of the requesting State through the same channel.

(2) Requests for mutual judicial assistance from foreign authorities to Cameroonian judicial authorities must be presented through diplomatic channels by the foreign Government concerned.

Enforcement documents shall be sent to the authorities of the requesting State through the same channel.

(3) In case of emergency, requests for judicial assistance from Cameroonian or foreign authorities may be sent directly to the authorities of the requested State for enforcement. The enforcement documents shall be dispatched to the relevant State authorities under the same conditions.

(4) Subject to international conventions, request for mutual judicial assistance from foreign authorities to Cameroonian judicial authorities shall be subject to an opinion of foreign Government concerned. Such opinion shall be forwarded to the relevant judicial authorities through diplomatic channels.

(5) In case of emergency, requests for mutual judicial assistance from foreign judicial authorities shall be forwarded to the State Counsel or Examining Magistrate with territorial jurisdiction.

(6) Where the State Counsel receives a request for mutual judicial assistance directly from authority, but which can only be enforced by the Examining Magistrate, he shall forward it to the latter for enforcement or refer to the General Prosecutor in the case provided for in section 94 below.

(7) Before proceeding to enforce a request for mutual assistance forwarded directly to him, the Examining Magistrate shall immediately communicate same to the State Counsel for an opinion.

Section 92. (1) Requests for mutual judicial assistance from foreign judicial officers shall be enforced by the State Counsel or Judicial Police Officers or Agents requested for this purpose by the said State Counsel.

(2) The requests shall be enforced by the Examining Magistrate or Judicial Police officers acting on the rogatory commission of the Examining Magistrate where they require certain procedural measures which can be ordered or enforced only during a preliminary investigation.

Section 93 (1) Request for mutual judicial assistance from foreign judicial officers shall be enforced in accordance with the procedure laid down by the Criminal Procedure Code.

(2) However, where the request for assistance so specifies, it shall be enforced in accordance with the procedure explicitly indicated by the relevant authorities of the requesting State, without such rules violating the rights of the parties or the procedural guarantees provided for by the Criminal Procedure Code.

(3) Where the request for mutual assistance cannot be enforced in accordance with the requirements of the requesting Sate, the relevant Cameroonian authorities shall immediately inform the authorities of the requesting State of such impossibility and specify under what conditions the request may be enforced.

(4) The relevant Cameroonian authorities and those of the requesting State may subsequently

agree on the onward processing of the request, where necessary, by subjecting it to compliance with such conditions.

(5) Irregularity in the transmission of the request for judicial assistance shall not constitute grounds for nullity of actions undertaken in enforcing such a request.

Section 94. (1) Where the enforcement of a request for judicial assistance from a foreign judicial authority is such as can breach public law and order or negatively affect the essential interests of the Nation, the State Counsel to whom the request is addressed or who is appraised thereof shall forward same to the General Prosecutor who shall transmit to the Minister in charge of Justice and where necessary, inform the State Counsel of such transmission.

(2) Where the request is forwarded to the Minister in charge of Justice, he shall inform the requesting authority, where necessary, that it is not possible to totally or partially accede to the request. Such information shall be communicated to the judicial authority concerned and shall block the enforcement of the request for mutual judicial assistance or the return of the enforcement papers.

PART V
TRANSITIONAL AND FINAL PROVISIONS

Section 95. The conditions of applications of this law shall, and as when necessary, be laid down by implementation instruments.

Section 96. Authorizations and declarations for the supply, import and export of cryptographic devices issued by the relevant authorities shall remain valid until the expiry of the time-limit specified therein.

Section 97. This law shall be registered, published according to the procedure of urgency and inserted in the Official Gazette in English and French.

Yaounde, 21 December 2010

(S) Paul Biya
President of the Republic