# Law N° 2010/021 of 21 December 2010 on Electronic Commerce 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 electronic commerce in Cameroon.**

**Section 2: For the purposes of this law and its implementing instruments, the following terms shall mean:**

**Commercial Activity:** Any activity for the production and exchange of goods and services carried out using electronic or material media, by any natural person or corporate body in accordance with the provisions of the laws, regulations and conventions governing trade;

**Certification Authority:** The body entrusted with the mission of generating and allocating public and private electronic keys and certificates;

**Electronic Certificate:** An electronic document protected by the electronic signature of the person who issued it and which attests, upon verification, to the authenticity of its content;

Qualified electronic Certificate: An electronic certificate issued by an authorized certification structure;

**Client:** Any natural person or corporate body using electronic means to conduct business with a trader;

**Electronic Commerce:** A commercial activity whereby a person uses electronic means to supply or ensure the supply of goods or services;

**Commercial Communication:** Any form of communication intended to directly or indirectly promote the goods, services or image of a company, an organization or an individual having a commercial, industrial, artisanal activity or engaged in a regulated profession;

**Consumer:** Any natural person or corporate body benefiting from the services or using commercial products to satisfy his personal needs or those of his dependants;

**Electronic Mail:** Any text, voice, audio or video message sent through a communication network, stored in a server of the network or in the terminal equipment of the addressee until the latter retrieves it;

**Service Addressee:** Any natural person or corporate body who, for professional purposes or otherwise, uses electronic means, in particular, to search for information or make it accessible;

Electronic signature generating system: All the equipment and/or private encrypting software approved by a competent authority, intended for the creation of electronic signatures;

Electronic signature verification system: All the equipment and/or public encrypting software authorized by a competent authority, which a certification authority uses to ascertain an electronic signature.

**Electronic Document:** All the data stored or saved in the memory of any media by a computer system or similar mechanism and which may be read or seen by a person or such a system or mechanism. This shall also include bill-posting and print-outs or any other such data;

Data relating to the creation of signatures: Unique data such as codes or private cryptographic keys, which the signatory uses to generate an electronic signature;

**Electronic Correspondence:** Exchanges conducted through electronic documents;

**Electronic Data Interchange (EDI):** Electronic transmission of information from computer to computer according to agreed standard rules for structuring information;

**Data Message:** Information created, sent, received or stored using electronic, optical or analog means, in particular, but not exclusively, the electronic data interchange (EDI), electronic messaging, telegraphy, telex and telecopy;

**Electronic means of payment:** Means enabling its holder to carry out distance payments through telecommunications networks;

**Electronic signature product:** Any material product, software or specific element of the said product, intended to be used by a certification service provider to deliver electronic signature services, or intended to be used in creating or verifying electronic signatures;

**Commercial Advertising:** Information published using various media to make a product or service known, with a view to encouraging the public to buy or use it;

**Electronic Signatory:** The person who owns a signature generating device and who acts either in his personal name or as a representative of a natural person or corporate body;

**Electronic Signature:** Signature obtained by an asymmetrical encryption algorithm that helps to authenticate the sender of a message and verify the integrity thereof;

**Information System:** Any isolated device or group of interconnected or linked devices, which ensure or one or more of whose elements ensure automated data processing according to a programme.

**Part II – Principles Governing the Exercice of Electronic Commerce-Related Activities**

**Chapter I – Restrictions and Exceptions**

**Section 3 (1):** The exercise of electronic commerce shall be free, to the exclusion:

- legally authorized money games, betting and lotteries;
- activities concerning legal representation and aid;
- activities carried out by notaries public.

(2) The exercise of electronic commerce shall be subject to compliance with the provisions relating to:

- conditions for setting up and operating an insurance business, as provided for under relevant international and national instruments;
- anti-trust practices and economic concentration;
- the prohibition or authorization of unsolicited advertising sent by electronic mail;
- the Customs Code of the Central African Economic and Monetary Community;
- the General Tax Code;
- rights protected by intellectual property laws and regulations.

**Section 4:** Under the conditions laid down by regulation, the administrative authority may, on a case by case basis, take restrictive measures on the free exercise of electronic commerce activities in case of disturbance or serious and great risk of undermining public order and security, the protection of minors, public health, defence of national interest or the protection of natural persons.

**Chapter II – Electronic Advertising**

**Section 5(1):** Any advertisement that is accessible through an online service shall slearly identify:

- the said advertisement;
- the natural person or corporate body for whom the advertisement is made;
- the promotional offers such as discounts, premiums or gifts, as well as competitions or promotional games, the conditions for participation of which shall be easily accessible, precise and unambiguous.

(2) The provisions of Section 5(1) shall apply without prejudice to the provisions that punish misleading advertising.

**Section 6:** Unsolicited advertising material made by a service provider by electronic mail shall be clearly and unequivocally identified once the addressee receives it.

**Section 7(1):** It shall be forbidden to engage in direct prospecting through a call processor, fax machine or an electronic mail using the address, in any form whatsoever, of a natural person or corporate body that has not expressed prior consent to receive direct prospecting by such means.

(2) Direct prospecting shall mean sending any message intended to directly or indirectly promote goods, services or the image of a person selling goods or providing services.

**Section 8 (1):** Members of regulated professions shall be authorized to use advertising in the exercise of their activities, subject to compliance with professional rules of independence, dignity and honour of the profession as well as confidentiality and loyalty to customers and the other members of the profession.

(2) Professional organizations and associations shall prepare the codes of conduct to specify the information which may be provided for advertising purposes in compliance with the rules referred to in Section 8(1) above.

**Chapter III – Contracts Signed by Electronic Means**

**Section 9:** The signing of contracts by electronic means shall be allowed subject to the conditions laid down by the laws and regulations in force.

**Section 10:** The regime of written contracts shall apply to electronic contracts in terms of consent, their legal effect, validity and implementation, except for the following contracts:

- contracts which create or transfer rights over immovable property, except for renting rights ;
- contracts for which the law requires the intervention of courts, public authorities or professions exercising public authority;
- surety and guarantee contracts produced by persons acting for purposes not coming under their professional or commercial activity;
- contracts governed by family law and succession law.

**Section 11 (1):** Bids made electronically concerning the supply of goods and services shall be accompanied by the contractual conditions applicable thereto such that they can be stored and reproduced. Without prejudice to the conditions of validity mentioned in the said bids, the authors of the bids shall remain bound as long as remaining accessible online is their own doing.

(2) The bids referred to in Section 11 (1) above shall clearly specify:

- the various steps to follow in concluding an electronic contract;
- the technical means that helps the user to spot any errors made in keying in data and to correct them before concluding the contract;
- the proposed language(s) for concluding the contract;
- in case of archiving the contract, the conditions for such archiving by the author of the bid and the conditions for accessing the contracts in the archives;
- the means for electronically consulting the professional and commercial rules which the author of the bid undertakes, where necessary, to abide by.

(3) The general contractual terms and conditions must be provided to the addressee such that it can keep and reproduce them.

(4) Sub-sections (1) and (2) of Section 11 above shall not apply to contracts signed exclusively through the exchange of electronic mail or though equivalent individual messages. There may also be exceptions to the provisions of the said sub-sections in agreements signed between professionals.

**Section 12 (1):** A contract may be deemed to be validly concluded only if the addressee of the bid previously had the possibility of verifying the details and total price of its order, and correcting any errors before confirming the bid to express acceptance.

(2) The author of the bid shall, within a period of no more than 5(five) days, acknowledge online receipt of the order addressed to it.

(3) The order, confirmation of acceptance of the bid and acknowledgement of receipt shall be deemed to have been received when the parties to which they are addressed can access them.

(4) Sub-sections (1) and (2) of Section 11 above shall not apply to contracts concluded exclusively through the exchange of electronic mail or through equivalent individual messages. There may also be exceptions to the provisions of the said sub-sections in agreements signed between professionals.

**Section 13 (1):** Where a paper document is required for the validity of a legal act, it may be issued and kept in an electronic form under the conditions stipulated in Sections 1317 et seq. of the Civil Code, relating to written proof.

(2) Where a handwritten note is required, even by the person making the undertaking, the latter may append the note electronically where the conditions for appending the note are such as to guarantee that it can be done solely by such person, except for the provisions of Section 13 (1) above for :

- private agreements relating to family law and succession law;
- private agreements relating to personal or real sureties, civil or commercial, save where they are signed by an individual for the purposes of its profession.

**Section 14:** Where the contract is concluded electronically and concerns an amount equal to or exceeding that fixed by regulation, the professional contracting party shall keep the ascertaining paper version for a period equally specified by regulation and ensure access thereto at all times by its contracting party if the latter so requests.

**Chapter IV – Electronic Commercial Transactions**

**Section 15 (1):** Prior to the conclusion of a contract, the seller shall be bound, during electronic commercial transactions, to provide the consumer with the following information in a clear and intelligible manner:

- the identity, address and telephone number of the seller or service provider;
- a complete description of the states for the conduct of the transaction;
- the nature, characteristic and price of the product;
- the cost of delivery and, where applicable, the insurance rates of the product and the required taxes;
- the duration of validation of the supply of the product at fixed prices;
- the conditions of commercial guarantees and after sales service;
- the payment conditions and procedures and, where applicable, the proposed credit conditions;
- the conditions and deadlines for delivery, execution of the contract and the consequences of failure to honour the commitments;
- the possibility of revocation and its timeframe;
- the procedure for confirming the order;
- the procedure for returning the product, change of product or refund;
- the cost of using telecommunication means where they are assessed using a reference other than the applicable rate;
- the conditions for terminating the contract where it is signed for an unspecified period or for a period of over 1 (one) year;
- the minimum contract period for contracts relating to long-term or periodic supply of a product or service.

(2) The information under sub-section (1) above must be provided electronically and put at the disposal of the consumer for consultation at all stages of the transaction.

**Section 16 (1):** It shall be prohibited for the seller to deliver a product not ordered by the consumer where it is accompanied by a request for payment.

(2) In case of delivery of a product not ordered by the consumer, the latter may not be requested to pay its price or the cost of its delivery.

(3) The cost of returning products delivered without any order shall be borne by the seller.

**Section 17:** Before concluding a contract, the seller shall allow the consumer to make a final statement of all its choices, confirm or modify the order as it may desire and consult the electronic certificate relating to its signing.

**Section 18:** Unless otherwise agreed by the parties, the contract shall be concluded at the address of the seller and on the date of acceptance of the order by the latter through an electronic document signed and addressed to the consumer.

**Section 19:** The seller shall have a period of 10

# Law N° 2010/021 of 21 December 2010 on Electronic Commerce in Cameroon

(ten) days with effect from the date of signature of the contract to provide the consumer, at the request of the latter, with a paper or electronic document containing all the information relating to the sales operation.

**Section 20 (1):** Subject to the provisions of section 15 above, the consumer may revoke its order within a period of 15 (fifteen) days :

- for goods, with effect from the day following the date the consumer receives them;
- for services, with effect from the date of conclusion of the contract.

(2) The revocation notice shall be transmitted electronically or by any other relevant means.

(3) Where the goods have not been damaged by the consumer, the seller shall be bound to refund the amount received within 15 (fifteen) days from the date of return of the goods or the revocation of the service.

(4) The consumer shall bear the cost of returning the goods.

**Section 21:** Subject to payment of damages to the consumer, the latter may, within 15 (fifteen) days of the date of delivery, return the product as it is where it does not meet the conditions of the order or where the seller has failed to deliver on schedule.

In such a case, the seller must refund the amounts received to the consumer within 15 (fifteen) clear days of the date of return of the product.

**Section 22:** Subject to Section 15 of this law and save in cases where the sales contract or the goods and services arising there from may contain obvious or hidden defects, the consumer may not renounce the order where it:

- requests the service to be delivered prior to the expiry of the deadline for revocation and the seller acted accordingly;
- receives products manufactured accordingly to personalized deteriorated or expired due to the expiry of the validity periods;
- detects delivered or downloaded audio or video recordings or computer software;
- buys newspapers and magazines.

**Section 23:** Where the sales operation is wholly or partially covered by a loan granted to the consumer by the seller or by a third party under a contract concluded between the seller and the third party, revocation by the consumer shall be tantamount to termination, without penalty, of the loan agreement.

**Section 24:** Save in cases of improper use, the seller shall bear, in case of sale after testing, the risks to which the product may be exposed and this, up to the end of the testing period of the product.

All disclaimer clauses repugnant to the provisions of this section shall be null and void.

**Section 25 (1):** Where the product or service ordered is unavailable, the seller shall inform the customer or consumer at least 24 (twenty-four) hours before the delivery date set in the purchase or service contract. Where applicable, the seller or service provider shall refund to the customer the total of amounts received for the delivery of the product or provision of the service.

(2) In case of force majeure, the contract shall be terminated where the seller fails to honour its commitments and the consumer shall be reimbursed all amounts paid, without prejudice to damages.

**Section 26:** The seller must prove the existence of prior information, confirmation of the information listed in Section 15 above, compliance with timeframes and the consent of the consumer. Any agreement repugnant hereto shall be null and void.

**Section 27:** Payment operations may be carried out in public services electronically under the conditions laid down by the laws and regulations in force.

**Section 28 (1) :** The holder of the electronic means of payment shall notify the issuer of the loss or theft of the said means or instruments used to operate it, as well as any fraudulent use it is aware of.

(2) The issuer of an electronic means of payment shall include the appropriate means for such notification in the contract concluded with its holder.

**Section 29(1):** Cases of fraud notwithstanding, the holder of the electronic means of payment shall :

- until notifies the issuer, assume responsibility for the loss or theft of the means of payment or the fraudulent use thereof by a third party;
- be released from all responsibility for the use of the electronic means of payment after notifying the issuer.

(2) The use of the electronic means of payment without presentation of the said means of payment and identification by electronic means shall not commit its holder.

## Part III – Responsibility of Service Providers and Intermediaries

### Chapter I – Obligation to Inform

**Section 30 (1) :** Without prejudice to other obligations to inform provided for by the laws and regulations in force, any person operating as a service provider in the domain of electronic commerce shall be bound to ensure that the end-users of the said service and the authorities have easy, direct and permanent access to the following minimum information:

- in case of a natural person, his/her full name and, in case of a corporate body, its company name, physical address, email address and its telephone number;
- where it is subject to the formalities for registration in the trade and personal property credit register, its registration number, its registered capital and head office address;
- where it is subject to the value added tax and identified by an individual number in keeping with Book I of the General Tax Code, its taxpayer's number;
- where its activity is subject to an authorization regime, the name and address of the authority that issued the authorization;
- where he/she is a member of a regulated profession, reference to the applicable professional rules, his/her professional title, the name and order or the professional organization to which he/she belongs.

(2) The obligations to inform and forward the contractual conditions referred to in Section 11 and Section 30 (1) above shall be fulfilled electronically in accordance with the conditions laid down by regulation.

**Section 31:** Subject to the conditions for setting rates and taxes under the laws and regulations in force, any person operating as a service provider in the domain of electronic commerce shall, even in the absence of an offer of contract, as long as he/she indicates a price, do so clearly and unequivocally and, in particular, where the delivery taxes and fees are included.

**Section 32:** Every service provider shall be bound to store and keep data relating to any commercial transaction carried out by electronic means in accordance with the laws and regulations in force.

### Chapter II – Storage, conservation and Transmission of Data

**Section 33:** Any natural person or corporate body engaged in automatic, intermediate and temporary storage for the sole purpose of making subsequent transmission of contents more efficiently shall not be criminally or vicariously liable for such contents, except in the following cases:

- it has modified the contents, failed to keep to their conditions for access and the usual rules for updating them or has obstructed the authorized and ordinary use of the technology used to obtain data;
- it has failed to act promptly to remove the contents he/she stored or make access thereto impossible, once it effectively became aware either of the fact that the contents transmitted initially have been removed from the network or due to the fact that it has become impossible to access the contents transmitted initially, either on account of the judicial authorities having ordered removal from the network of the contents transmitted initially or denial of access thereto.

**Section 34(1):** The electronic document shall be stored on an electronic medium making it possible to:

- consult its content throughout its validity period;
- keep it in its final form in order to ensure the integrity of its content, conserve the information relating to its provenance and destination as well as the date and place of its issuance or reception.

(2) The conservation of the electronic document as well as that of the paper document shall be authentic.

(3) The issuer shall undertake to keep the electronic document in the format in which it was issued. The addressee shall undertake to keep the electronic document in the format in which it is received.

## Part IV – Securing and Authentication of Data and Information

### Chapter I – Electronic Certificate and Signature

**Section 35 (1):** Any natural person or corporate body shall be authorized to use the electronic certificate and signature in electronic commerce under the conditions laid down by a separate instrument.

(2) Official documents may be authenticated in government services using electronic certificates and signatures under conditions laid down in separate instruments.

**Section 36:** Anyone using an electronic signature device shall:

- take the minimum precautionary measures set forth in the instruments in force to avoid any unauthorized use of the personal equipment concerning its signature;
- report any unauthorized use of its signature to the certification authority;
- ensure the accuracy of all the information it provides to the said authority;
- ensure the veracity of all the information it provided to any person whom it has asked to rely on its signature.

**Section 37 :** In case of violation of the provisions of Section 36 above, the holder of the signature shall be held responsible for the tort caused another person.

**Section 38:** The conditions for exercising the activities of certification authority shall be laid down in a separate instrument.

**Section 39:** The certification authority shall keep an electronic register of certificates at the disposal of users.

### Chapter II – Equivalences

**Section 40 (1):** The certificates and signatures issued by a certification authority based abroad shall have the same value as those issued by a certification authority based in Cameroon, where such an authority is recognized under a mutual recognition agreement signed by the competent authorities of the States concerned.

(2) The conditions for the legal recognition of electronic certificates and signatures issued from third countries shall be defined in a separate instrument by default.

## Part V – Establishing Offences and Penalties

**Section 41 (1):** All violations of the provisions of this law and its implementing instruments shall be established by criminal investigation officers with general jurisdiction, sworn officers of the Ministries in charge of telecommunications and advertising, the electronic regulation and certification authority, as well as those of economic control, in accordance with the conditions set forth in the laws and regulations in force.

(2) Reports establishing offences as well as objects and documents seized shall be transmitted to the State Counsel with territorial jurisdiction.

**Section 42:** Whoever illegally uses the electronic signature of another shall be punished with the penalties provided in Section 219 of the Penal Code.

**Section 43:** Whoever is found guilty of breaching the provisions of Section 15, 17, 19, 21, 24 and 25 of this law shall be punished with a fine of from 250 000 to 2 500 000 FCFA francs.

**Section 44 :** Whoever takes advantage of the weakness or ignorance of another to make him/her enter, through an electronic sale, into commitments in cash or on credit in any form whatsoever, where it is proven that such a person is not capable of appreciating the extent of the commitments he/she is making or detecting the trick or tactics being used to convince him/her to subscribe thereto or that he/she was under duress shall be punished with the penalties set forth in Section 349 of the Penal Code.

**Section 45 :** The certification authority and/or its officers who disclose, cause or participate in the disclosure of information entrusted to them within the framework of the exercise of their activities shall be punished with the penalties provided in Section 310 of the Penal Code, except for those whose publication or communication are authorized by the older of the certificate either in writing, by electronic means or in the cases provided by the law in force.

**Section 46:** Any violation of the provisions of Sections 9 and 10 of this law shall be punished with the penalties set forth in Sections 37 and 38 of Law No. 90/31 of 10 August 1990 governing commercial activity.

## Part VI – Transitional and Final Provisions

**Section 47:** Any natural person or corporate body engaged in electronic commerce on the date of enactment of this law shall have a period of 6 (six) months within which to comply with provisions.

**Section 48:** 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**

**Paul BIYA**

**President of the Republic**

# Un enfant retrouvé et pris en charge par le MINAS

## Le communiqué parvenu à notre Rédaction

Le ministre des Affaires sociales a l'honneur de porter à la connaissance de l'opinion publique, que dans le cadre de La protection sociale de l'enfant, un enfant en détresse retrouvé abandonné, a été conduit dans les services opérationnels du MINAS.

Cet enfant qui continue de faire l'objet de recherche de sa famille sur l'ensemble du territoire national, est actuellement pris en charge nutritionnelle, sanitaire et psychosociale dans les structures spécialisées de son département ministériel.

Il s'agit :

- d'un enfant de sexe masculin, âgé aujourd'hui d'environ 5 ans, répondant au nom de Nyobe Alain Joël, retrouvé le 9 décembre 2010.

Les parents ou famille de cet enfant, et toute personne qui se sentirait concernée sont invités à prendre attache avec les services déconcentrés locaux et/ou centraux du ministère des Affaires sociales sis derrière l'ancien palais présidentiel ou appeler au 22 22 29 58, 22 23 05 35 ou 74 88 69 04 ou écrire à minascab@yahoo.fr.

Le ministre des Affaires sociales prie par ailleurs lesdits parents ou relatifs de bien vouloir se munir de tout document permettant d'établir l'existence d'un lien de filiation ou de toute autre relation avec l'enfant afin de procéder à son retour en famille.

**Pour le ministre des Affaires sociales et par délégation, le secrétaire général,**
**(é) MOUHTAR OUSMANE**
**Administrateur civil principal**

Cameroon tribune

# Loi n° 2010/012 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité au Cameroun

L'Assemblée Nationale a délibéré et adopté, le président de la République promulgue la loi dont la teneur suit :

**Titre premier : Dispositions générales**

**Article 1er : -** La présente loi régit le cadre de sécurité des réseaux de communications électroniques et des systèmes d'information, définit et réprime les infractions liées à l'utilisation des technologies de l'information et de la communication au Cameroun.

A ce titre, elle vise notamment à :

Instaurer la confiance dans les réseaux de communications électroniques et les systèmes d'information ;

Fixer le régime juridique de la preuve numérique, des activités de sécurité, de cryptographie et de certification électronique ;

Protéger les droits fondamentaux des personnes physiques notamment le droit à la dignité humaine, à l'honneur et au respect de la vie privée, ainsi que les intérêts légitimes des personnes morales.

**Art. 2. –** Sont exclues du champ de la présente loi, les applications spécifiques utilisées en matière de défense et de sécurité nationale.

**Art. 3.-** Les réseaux de communications électroniques visés par la présente loi comprennent : les réseaux satellitaires, les réseaux terrestres, les réseaux électroniques lorsqu'ils servent à l'acheminement de communications électroniques, les réseaux assurant la diffusion ou la distribution de services de communications audiovisuelles.

**Art. 4.-** Au sens de la présente loi et de ses textes d'application, les définitions ci-après, sont admises :

**Accès illicite** : accès intentionnel, sans en avoir le droit, à l'ensemble ou à une partie d'un réseau de communications électroniques, d'un système d'information ou d'un équipement terminal ;

**Administration chargée des Télécommunications** : ministère ou ministre, selon les cas, investi pour le compte du gouvernement, d'une compétence générale sur le secteur des télécommunications et des technologies de l'information et de la communication ;

**Algorithme** : suite d'opérations mathématiques élémentaires à appliquer à des données pour aboutir à un résultat désiré ;

**Algorithme asymétrique** : algorithme de chiffrement utilisant une clé publique pour chiffrer et une clé privée (différente) pour déchiffrer les messages ;

**Algorithme symétrique** : algorithme de déchiffrement utilisant une même clé pour chiffrer et déchiffrer les messages ;

**Attaque active** : acte modifiant ou altérant les ressources ciblées par l'attaque (atteinte à l'intégrité, à la disponibilité et à la confidentialité des données) ;

**Attaque passive** : acte n'altérant pas sa cible (écoute passive, atteinte à la confidentialité) ;

**Atteinte à l'intégrité** : fait de provoquer intentionnellement une perturbation grave ou une interruption de fonctionnement d'un système d'information, d'un réseau de communications électroniques ou d'un équipement terminal, en introduisant, transmettant, endommageant, effaçant, détériorant, modifiant, supprimant ou rendant inaccessibles des données ;

**Audit de sécurité** : examen méthodique des composantes et des acteurs de la sécurité, de la politique, des mesures, des solutions, des procédures et des moyens mis en œuvre par une organisation, pour sécuriser son environnement, effectuer des contrôles de conformité, des contrôles d'évaluation de l'adéquation des moyens (organisationnels, techniques, humains, financiers) investis au regard des risques encourus, d'optimisation, de rationalité et de performance ;

**Authentification** : critère de sécurité défini par un processus mis en œuvre notamment pour vérifier l'identité d'une personne physique ou morale et s'assurer que l'identité correspond à l'identité de cette personne préalablement enregistrée ;

**Autorité de certification** : autorité de confiance chargée de créer et d'attribuer des clés publiques et privées ainsi que des certificats électroniques ;

**Autorité de Certification Racine** : organisme investi de la mission d'accréditation des autorités de certification, de la validation de la politique de certification des autorités de certification accréditées, de la vérification et de la signature de leurs certificats respectifs ;

**Certificat électronique** : document électronique sécurisé par la signature électronique de la personne qui l'a émis et qui atteste après constat, la véracité de son contenu ;

**Certificat électronique qualifié** : certificat électronique émis par une autorité de certification agréée ;

**Certification électronique** : émission de certificats électroniques ;

**Chiffrement** : procédé grâce auquel on transforme à l'aide d'une convention secrète appelée clé, des informations claires en informations intelligibles par des tiers n'ayant pas la connaissance de la clé ;

**Clé** : dans un système de chiffrement, elle correspond à une valeur mathématique, un mot, une phrase qui permet, grâce à l'algorithme de chiffrement, de chiffrer ou de déchiffrer un message ;

**Clé privée** : clé utilisée dans les mécanismes de chiffrement asymétrique (ou chiffrement à clé publique), qui appartient à une entité et qui doit être secrète ;

**Clé publique** : clé servant au chiffrement d'un message dans un système asymétrique et donc librement diffusé ;

**Clé sécrète** : clé connue de l'émetteur et du destinataire servant de chiffrement et de déchiffrement des messages et utilisant le mécanisme de chiffrement symétrique ;

**Code source** : ensemble des spécifications techniques, sans restriction d'accès ni de mise en œuvre, d'un logiciel ou protocole de communication, d'interconnexion, d'échange ou d'un format de données ;

**Communication audiovisuelle** : communication au public de services de radiodiffusion télévisuelle et sonore ;

**Communication électronique** : émission, transmission ou réception de signes, signaux, d'écrits, d'images ou de sons, par voie électromagnétique ;

**Confidentialité** : maintien du secret des informations et des transactions afin de prévenir la divulgation non autorisée d'informations aux non destinataires permettant la lecture, l'écoute, la copie illicite d'origine intentionnelle ou accidentelle durant leur stockage, traitement ou transfert ;

**Contenu** : ensemble d'informations relatives aux données appartenant à des personnes physiques ou morales, transmises ou reçues à travers les réseaux de communications électroniques et les systèmes d'information ;

**Contenu illicite** : contenu portant atteinte à la dignité humaine, à la vie privée, à l'honneur ou à la sécurité nationale ;

**Courrier électronique** : message, sous forme de texte, de voix, de son ou d'image, envoyé par un réseau ou dans l'équipement terminal du destinataire, jusqu'à ce que ce dernier le récupère ;

**Cryptage** : utilisation de codes ou signaux non usuels permettant la conservation des informations à transmettre en des signaux incompréhensibles par les tiers ;

**Cryptanalyse** : ensemble des moyens qui permet d'analyser une information préalablement chiffrée en vue de la déchiffrer ;

**Cryptogramme** : message chiffré ou codé ;

**Cryptographie** : application des mathématiques permettant d'écrire l'information, de manière à la rendre inintelligible à ceux ne possédant pas les capacités de la déchiffrer ;

**Cybercriminalité** : ensemble des infractions s'effectuant à travers le cyberspace par des moyens autres que ceux habituellement mis en œuvre, et de manière complémentaire à la criminalité classique ;

**Cybersécurité** : ensemble de mesures de prévention, de protection et de dissuasion d'ordre technique, organisationnel, juridique, financier, humain, procédural et autres actions permettant d'atteindre les objectifs de sécurité fixés à travers les réseaux de communications électroniques, les systèmes d'information et pour la protection de la vie privée des personnes ;

**Déclaration des pratiques de certification** : ensemble des pratiques (organisation, procédures opérationnelles, moyens techniques et humains) que l'autorité de certification compétente applique dans le cadre de la fourniture de ce service et en conformité avec la (les) politique (s) de certification qu'elle s'est engagée(s) à respecter ;

**Déchiffrement** : opération inverse du chiffrement ;

**Déni de service** : attaque par saturation d'une ressource du système d'information ou du réseau de communications électroniques, afin qu'il s'effondre et ne puisse plus réaliser les services attendus de lui ;

**Déni de service distribué** : attaque simultanée des ressources du système d'information ou du réseau de communications électroniques, afin de les saturer et amplifier les effets d'entrave ;

**Disponibilité** : critère de sécurité permettant que les ressources des réseaux de communications électroniques, des systèmes d'information ou des équipements terminaux soient accessibles et utilisables selon les besoins (le facteur temps) ;

**Dispositif de création de signature électronique** : ensemble d'équipements et/ou logiciels privés de cryptage, homologués par une autorité compétente, configurés pour la création d'une signature électronique ;

**Dispositif de vérification de signature électronique** : ensemble d'équipements et/ou logiciels publics de cryptage, homologués par une autorité compétente, permettant la vérification par une autorité de certification d'une signature électronique ;

**Données** : représentation de faits, d'informations ou de notions sous une forme susceptible d'être traitée par un équipement terminal, y compris un programme permettant à ce dernier d'exécuter une fonction ;

**Données de connexion** : ensemble de données relatives au processus d'accès dans une communication électronique ;

**Données de trafic** : donnes ayant trait à une communication électronique indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type du service sous-jacent ;

**Equipement terminal** : appareil, installation ou ensemble d'installations destiné à être connecté à un point de terminaison d'un système d'information et émettant, recevant, traitant, ou stockant des données d'information ;

**Fiabilité** : aptitude d'un système d'information ou d'un réseau de communications électronique à fonctionner sans incident pendant un temps suffisamment long ;

**Fournisseur des services de communications électroniques** : personne physique ou morale fournissant les prestations consistant entièrement ou principalement en la fourniture de communications électroniques ;

**Gravité de l'impact** : appréciation du niveau de gravité d'un incident, pondéré par sa fréquence d'apparition ;

**Intégrité des données** : critère de sécurité définissant l'état d'un réseau de communications électroniques, d'un système d'information ou d'un équipement terminal qui est demeuré intact et permet de s'assurer que les ressources n'ont pas été altérées (modifiées ou détruites) d'une façon tant intentionnelle qu'accidentelle, de manière à assurer leur exactitude, leur fiabilité et leur pérennité ;

**Interception illégale** : accès sans en avoir le droit ou l'autorisation, aux données d'un réseau de communications électroniques, d'un système d'information ou d'un équipement terminal ;

**Interception légale** : accès autorisé aux données d'un réseau de communications électroniques, d'un système d'information ou d'un équipement terminal ;

**Intrusion par intérêt** : accès intentionnel et sans droit dans un réseau de communications électroniques ou dans un système d'information, dans le but soit de nuire soit de tirer un bénéfice économique, financier, industriel, sécuritaire ou de souveraineté ;

**Intrusion par défi intellectuel** : accès intentionnel et sans doit dans un réseau de communications électroniques ou dans un système d'information, dans le but de relever un défi intellectuel pouvant contribuer à l'amélioration des performances du système de sécurité de l'organisation ;

**Logiciel trompeur** : logiciel effectuant des opérations sur un équipement terminal d'un utilisateur sans informer préalablement cet utilisateur de la nature exacte des opérations que ce logiciel va effectuer sur son équipement terminal ou sans demander à l'utilisateur s'il consent à ce que le logiciel procède à ces opérations ;

**Logiciel espion** : type particulier de logiciel trompeur collectant les informations personnelles (sites web les plus visités, mots de passe, etc.) auprès d'un utilisateur du réseau de communications électroniques ;

**Logiciel potentiellement indésirable** : logiciel représentant des caractéristiques d'un logiciel trompeur ou d'un logiciel espion ;

**Message clair** : version intelligible d'un message et compréhensible par tous ;

**Moyen de cryptographie** : équipement ou logiciel conçu ou modifié pour transformer des données, qu'il s'agisse d'informations ou de signaux, à l'aide de conventions secrètes ou pour réaliser une opération inverse avec ou sans convention secrète afin de garantir la sécurité du stockage ou de la transmission de données, et d'assurer leur confidentialité et le contrôle de leur intégrité ;

**Non répudiation** : critère de sécurité assurant la disponibilité de preuves qui peuvent être opposées à un tiers et utilisées pour prouver la traçabilité d'une communication électronique qui a eu lieu ;

**Politique de certification** : ensemble de règles identifiées, définissant les exigences auxquelles l'autorité de certification se conforme dans la mise en place de ses prestations et indiquant l'applicabilité d'un service de certification à une communauté particulière et/ou à une classe d'applications avec des exigences de sécurité communes ;

**Politique de sécurité** : référentiel de sécurité établi par une organisation, reflétant sa stratégie de sécurité et spécifiant les moyens de la réaliser ;

**Prestation de cryptographie** : opération visant à la mise en œuvre, pour le compte d'autrui, de moyens de cryptographie ;

**Réseau de communications électroniques** : système de transmission, actif ou passif et, le cas échéant, les équipements de commutation et de