THE REALISATION OF THE RIGHT TO PRIVACY IN THE CAMEROON ELECTRONIC COMMUNICATION SECTOR

Written by ***Masah Tise Vigiline***

Ph.D. in Law, Department of English Law, Faculty of Laws and Political Science, University of Buea, Buea, Cameroon

ABSTRACT

Each individual has the right to decide about what he/she wants the outside world to know about him/her but modern technologies pose a serious threat to the privacy of individuals. In order to preserve the private life on individuals, national and international instruments have been signed and ratified by Cameroon in which they recognise that every adult and children have the right to their privacy. At the same time, other instruments recognise the fact that every individual has the right to benefit from electronic communication services. With the use of electronic communication tools, people's privacy is at stake and government has the obligation to take necessary measures to preserve citizen's privacy. Cameroonian instruments do not give a clear definition of what is meant by privacy. However, from the deduction of the various instruments governing the electronic communication sector, privacy can be considered to mean the confidentiality and respect of the principle of inviolability and secrecy of messages transferred through electronic communication networks, the protection of consumers' personal data and the security of information transferred through electronic communication and information systems. As such violation of privacy in the Cameroon electronic communication sector is the unauthorised interception or transmission of personal data, information and correspondence as well as the violation and unaunthorised publication or transmission of information that can be prejudicial to an individual's dignity and integrity, added to the injury of a child's honour and self-respect. In order to avoid such violation, Cameroonian government has taken a series of administrative, preventive and defensive measures. The aim of these

measures is to deter and punish anyone who violates an individual's or a child's right to privacy. Consequently, a good number of institutions have been put in place to ensure the realization of the right to privacy in the electronic communication sector. Acts considered as violation well as their respective punishments have equally been listed under panoply of legal instruments. The legislator has stated the procedure to be followed both at the national and international level to ensure that those who violate the right to privacy should not go unpunished.

Keywords- Respect, Protection, Fulfilment, Right to Privacy, Data protection, Confidentiality of Information and Messages, Electronic Communication Sector

RECOGNITION OF THE RIGHT TO PRIVACY IN THE CAMEROON ELECTRONIC COMMUNICATION SECTOR

According to Charles Fried and Alan Westin, privacy is *'the control we have over information about ourselves'*[i] and *'the claim of an individual to determine what information about* him /her *should be known to others.* [ii] For Hajdu, privacy is an environment around an individual, which constitutes the limit between himself and the outside world.[iii] The right to privacy is considered by Warren and Brandies as the right to be let alone and they recognise technological development as one of the phenomena that pose a threat to privacy.[iv] In Cameroon, the right to privacy is recognized in global, regional and in national instruments.

Internationally, both adults and children have the right to their privacy as guaranteed under the various instruments ratified by Cameroon. Concerning adults, their right to privacy is contained in article 12 of the Universal Declaration of Human rights, article 17 of the International Covenant on Civil and Political Rights (ICCPR) and article 14 of the International Convention on the Protection of Migrant Workers and Members of their Families[v]. All these articles provide that no individual *'...shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, or other communications, nor to unlawful attacks on*

his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.'

As far as children are concerned, their right to privacy is guaranteed in article 16 of the International Convention on the Rights of a Child[vi] and article 10 of the African Charter on the Rights and Welfare of the Child.[vii] Though the right to privacy does not feature in the African Charter on Human and Peoples' Rights[viii], the International Convention and African charter on the rights and welfare of the Child consecrates children's rights to privacy. These international instruments forbid the act of subjecting a child to an unlawful or arbitrary interference with his privacy, home, family or correspondence. In other words, no one is authorised to violate a child's privacy, home, family or correspondence. No one is equally authorised to tarnish a child's honour and reputation on condition that his/her parents or legal guardians should be allowed to exercise reasonable supervision over the child's behaviour.

In addition to the above-mentioned instruments, we have the CEMAC Directive No 07/08-UEAC-133-CM-18 laying down the legal framework for the protection of the rights of users of the electronic communication services in the CEMAC region.[ix] Article 3 of this directive is to the effect that member states shall ensure the protection of the privacy of users by ensuring the confidentiality electronic communications and traffic. As such everyone is forbidden from listening, intercepting or storing communications and data, or enabling such interception or surveillance without the author's consent.

Concerning national instruments, the right to privacy is recognised in the Cameroon Constitution[x] and other legal instruments. The Preamble of the Cameroon Constitution guarantees the right to privacy by providing the inviolability of the home as well as forbids arbitrary searches. It equally provides for the inviolability of the privacy of all correspondence and forbids any interference by whosoever except by virtue of decisions emanating from the Judicial Power. Article 45 goes further to state that duly ratified Treaties, Conventions and International agreements override the laws of Cameroon. As such, the Constitution expressly recognises all international instruments guaranteeing the right to privacy that Cameroon has signed and ratified.

The right to privacy is equally enshrined in law n° 2010/012 of 21 December 2010 relating to cybersecurity and cyber criminality in Cameroon.[xi] It states that *'every individual shall have the right to the protection of their privacy."* Decree No 2013/0399/PM of 27 February 2013 on the modalities of the consumers' protection in the electronic communication sector states that *"consumers in the electronic communication sector have the right to privacy ... in the consumption of technologies, goods and services in the electronic communication sector;"*[xii]

Generally, the right to privacy is recognized both in human rights instruments and in instruments governing the electronic communication sector in the CEMAC sub-region as well as in Cameroon. A problem that may occur at this level is the meaning of privacy in the electronic communication sector in Cameroon. This is the reason why the determination of the meaning of this right in the said sector is a prerequisite to the examination of the various measures put in place to ensure its realization.

THE CONTENT OF PRIVACY IN THE CAMEROON ELECTRONIC COMMUNICATION SECTOR

The 2010 law governing electronic communications in Cameroon[xiii] states that every individual has the right to benefit from electronic communication services no matter where he/she is located on the national territory.[xiv] Electronic communications is defined as the *"emission, transmission or reception of signs, signals, writings, images or sounds through electronic means."*[xv] The latter include email, facsimile transmission, internet, telex, telegraph, telecopy, including a telephone communication confirmed by writing.[xvi] This law does not provide a clear definition of what is meant by privacy but the latter can be considered to have a great link with human dignity and character.[xvii]

According to the wordings of the above mentioned CEMAC Directive,[xviii] it can be deduced that privacy in the electronic communications sector entails communications and data exchanged through electronic means.[xix] The provisions of this legal instrument is

complemented by those of the 2010 law on electronic communications[xx] which punishes anyone who intercepts and discloses a private conversation, be it voluntarily or involuntarily without the consent of the author.

As earlier mentioned, though the above mentioned instruments do not clearly state what is meant by privacy in the electronic communication sector in Cameroon, the 2013 Decree on consumers' protection in this sector states that the right to privacy entails the *"confidentiality and respect of the principle of inviolability and secrecy of messages transferred through electronic communication networks, the protection of consumers' personal data and the security of information transferred through electronic communication and information systems".*[xxi] This could be interpreted to mean that as far as consumers are concerned, the violation of their privacy has to do with the violation of the confidentiality of their messages or correspondence, data and information exchanged through electronic means.

In the same light, the law on cybersecurity and cyber criminality lays down a good number of things, including personal data, which if carried out, will be considered to be in violation of privacy. Some of these are the disclosure of personal information that undermines the consideration due to the victim, images that undermine the bodily integrity of another person, the design, act or publication of a child's pornography message or a message likely to seriously injure the self-respect of a child, publication of acts of indecency, etc.[xxii]

To sum this up, the violation of privacy in the electronic communication sector can be considered to be the unauthorized interception or transmission of personal data, information and correspondence as well as the violation and unauthorized publication or transmission of information that can be prejudicial to an individual's dignity and integrity, added to the injury of a child's honour and self-respect. It is important to note that these acts must have been carried out using electronic means of communications. In order to deter the violation of this right, Cameroon government has put in place a series of measures to ensure the realization of the right to privacy in the electronic communication sector.

MEASURES PUT IN PLACE FOR THE REALISATION OF PRIVACY IN CAMEROON

Under international human rights law, the state has the obligation to realize every individual's right to privacy.[xxiii] In order to do so, it has the obligation to respect, protect and fulfill this right. Respecting the right to privacy requires the state to refrain from interfering directly or indirectly with the right to privacy.[xxiv] The state protects this right by preventing third parties from interfering with the right to privacy.[xxv] It fulfills this right by adopting appropriate measures to guarantee this right. As such, the state has to put in place preventive and repressive measures to ensure the realization of the right to privacy.[xxvi]

Preventive Measures

With regard to preventive measures, a good number of legislative measures have been put in place to ensure the realization of the right to privacy in the electronic communication sector in Cameroon. As stated above, Cameroon government has ratified treaties and conventions that guarantee the right to privacy not only in the electronic communication sector but for every human being notwithstanding whether he/she is a consumer of the information communication technology or not. Government has equally signed several national instruments to ensure the promotion and protection of this right in this sector. During this electronic period of the information and communication technology, much personal information is shared over social media and it is argued that the right to privacy is now a myth.[xxvii] In order to ensure the respect of individuals' privacy, Cameroon government has enacted a series of laws and regulations recognizing and guaranteeing the respect of the right to privacy.

In addition to the above-mentioned laws recognizing the right to privacy in Cameroon, the 2010 Law on Cyber security and Cyber Criminality states that every individual shall have the right to the protection of their privacy. It gives Judges the power to take any protective measures such as sequestration or seizure to avoid or end the invasion of privacy.[xxviii] It gives Judges the authorization to take such measures in order to protect, prevent or stop the violation of an individual's right to privacy. This law goes further to ensure that information channeled through electronic communication networks shall be made confidential by operators of this

system. More to that, it makes content providers responsible for data transmitted through their systems, if the content of such information violates, infringes or invades an individual's privacy.[xxix] In order to ensure the inviolability of the right to privacy, they are bound to set up liters in order to contain any attacks that may be prejudicial to the personal data in privacy of users.[xxx]

Equally, the law on cybersecurity and criminality forbids natural persons and corporate bodies from listening, intercepting, monitoring and storing communications without the consent of the users concerned, except where such person is legally authorized to do so. However, the same law states that criminal investigation officers may intercept record or transcribe any electronic communication in case of crimes or offences provided for hereunder.[xxxi]

In line with the provisions of the Law on Cyber security and Cyber Criminality, the provisions of the law regulating electronic communications in Cameroon states that *'operators shall take every necessary measures to ensure the protection of individual's privacy.'*[xxxii] *This law equally states '…that persons whose activity consists in providing access to electronic communication services, and those 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 shall be bound by confidentiality. In case of any violation, they shall be liable.'*[xxxiii] Equally, their responsibility may not be engaged if they were not aware of the illicit nature of the facts or circumstances characterizing them as such, and if they proceed to the immediate withdrawal or ensuring its inaccessibility once they become aware of the fact the information is illicit.[xxxiv]

Moreover, they shall equally be responsible for data transmitted through their information system especially, if such content may cause the violation of human dignity, injury to character and invasion of privacy.[xxxv] As such, content and access providers are in charge of keeping data safe and ensuring that no one uses such data to violate an individual's dignity, character and privacy. To this effect, they shall be bound to set up liters in order to contain any attacks that may be prejudicial to the personal data in users' privacy.[xxxvi]

Equally, the law forbids an individual or a company from listening, intercepting and storing communications as well as transferring data related thereto, or subjecting same to any other means of interception or monitoring without the consent of the users concerned, except where such person is so authorized legally.[xxxvii] More to that, any sender whose aim is to do advertisement is prohibited from dissimilating his identity before sending an electronic message. He is equally prohibited from sending such message without indicating the valid address to which the addressee may send a request aimed at blocking such information. Usurping another user's identity to send an electronic mail is also prohibited[xxxviii].

However, it is important to note that though this law goes a long way to deter potential violators of the right to privacy, it equally gives room for such violation by stating that *'…confidentially can be breached if the information is requested by a judicial authority.'*[xxxix] This could be interpreted to mean that though government has the duty to respect, protect and fulfill the right to privacy in the electronic communication sector, it strives to protect such right but opens the door for her agents not respect and ensure the realization of this right. In order words, giving the possibility for judicial authorities and judges to violate the confidentiality of individuals' right to privacy is opening the door for judicial authorities to violate the right at their own pace and will. By so doing, they are violating their duty to respect this right.

Again, in order to protect individual's privacy, consumers are given the possibility of hiding their numbers. Content and service providers are forbidden from using a consumer's electronic communications without his/her consent.[xl] They are equally forbidden from permitting the publication of prospective network messages through their network without the publisher's identity.

These provisions are laid down to deter service providers who may for one reason or the other want to use an individual's message for business purposes without the author's knowledge and/or indirectly having benefits from an individual's message and at the same not wanting the author to know who is taking advantage of him. However, such direct prospection can be allowed if the information published is obtained directly from the consumer himself though the

latter should put into place a free means enabling the receiver to end the prospection at any moment.[xli]

Administrative Measures

As far as administrative measures are concerned, government has put in place effective regulatory institutions in the electronic communications sector to ensure monitoring the activities of service providers and users in a bit to ensure the respect of the right to privacy. Some of these institutions include the Ministry of Post and Telecommunication, the Telecommunication Regulatory Board, the National Telecommunication Agency and the National Communication Council.

Ministry of Post and Telecommunication (MINPOSTEL)

As laid down in article 1 of Decree No 2005/124 of 15 April 2005 on the organization and functioning of the Ministry of Posts and Telecommunications, this ministry is placed under the authority of a Minister and is responsible for the development and implementation of government's posts, telecommunications, and IC technologies. In the electronic communication sector, it carries out the following functions:

- It ensures the development of ICT, as well as electronic communications in all their forms, in conjunction with the administrations concerned;
- It monitors the activities of mobile or satellite telecommunications companies;
- It monitors the activities relating to e-commerce and issues of cybercrime in conjunction with the administrations concerned;
- It monitors the activities or regulatory bodies operating in his sector of competence;
- It supervises the activities of:

  -the Telecommunication Regulatory Board;

  - the National Agency for Information and Communications Technology

  -the CAMPOST, CAMTEL and the National Advanced School of Post and Telecommunications.

By virtue of Section 6 of the 2010 law on Cybersecurity and cyber criminality, 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. In a bit to ensure the respect of privacy in the electronic communication sector, it monitors the evolution of issues related to security and ensures the protection of consumers in the electronic communication sector.

National Telecommunications Agency (NAICT)

The NAICT is the Internet and ICT Regulator in Cameroon. It is a public Administrative establishment with legal personality and financial autonomy. It is placed under the Ministry of posts and Telecommunications and the financial supervision of the Ministry of Finance.
The NAICT regulates the activities of electronic certification and regulation of the internet in Cameroon.[xlii] Besides its mission of the promotion and follow up of the action of public authorities in ICT, it is responsible for the regulation of electronic security activities in collaboration with the Telecommunications Regulatory Board.[xliii] It is responsible for ensuring the use of ICT with respect to ethics, as well as the protection of intellectual property, privacy, consumers, and morality.

- Implement mechanisms to resolve disputes on the one hand, between ICT operators and secondly, between operators and users, for problems specifically related to the content and quality of services (scamming, phishing, hacking);
- Put in place mechanisms to ensure internet security at the national level;
- monitor, detect and provide information on computer-related risks and cybercriminal activities;

The NAICT has put in place a privacy policy to ensure the protection of individual's personal information in the electronic communication sector. It can only reveal or provide a customer's personal information to third parties with the customer's consent. In order to obtain a customer's consent, it goes through a procedure called *'the member consent request procedure'* whereby it informs customers of the purpose, content and the reason why it has to reveal or share such information. If the subscriber does not consent, the information cannot be shared.

If the information to be shared goes beyond the scope previously agreed on, it can go through another procedure named, *'separate consent request procedures'* to seek for authorization to exceed this scope. Moreover, customers have the possibility of cancelling their consent if they no longer wish that that their personal information should be shared. If the customer subsequently decides to cancels his consent, the NAICT will requests that the relevant Corporation should delete the corresponding personal information.

However, there are situations where personal information can be provided without a subscriber. These situations must be in accordance with relevant laws and must only be when requested by government institutions, the Information & Communication Ethics Committee for criminal investigations, and when required to settle charges, and provided after processing so that a specific individual may remain anonymous.

It is important to note that with the aim of protecting personal information, the NAICT has put in place the *'Personal information protective measures*. Through these measures, it uses a firewall (invasion quarantine system) to block the theft, leak, forgery, deformation of personal information by cracking (malicious hacking) and so on.[xliv] The firewall is installed on each server and in the network to track illegal invasions 24 hours a day. They regularly back up the subscriber's personal information to prepare against any possible accidents. In addition, it has minimized and controls staff handling personal information, and takes corrective actions immediately when any problem is found. It also does its utmost to take technical and administrative measures to prevent customers' personal information from leaking. The subscriber can access their personal information using their password and can modify their own personal information using the membership ID and password. Therefore, the customer must ensure that this password is not revealed to other persons. The customer is liable for membership ID, password, and personal information leaks. As such, the NAICT does not take any responsibility unless there is liability attributable.[xlv]

National Communication Council (NCC)

The National Communication Council is a regulatory and consultative body with legal personality and financial autonomy. Created by Law No 90/052 of 19 December 1990 on the freedom of social communication, its organization and functioning are governed by Decree No 2012/038 of 23 January 2012 reorganizing the National Communication Council.

As far as its rules and missions are concerned, the NCC ensures that its decisions and opinions are respected. It ensures the respect of laws and regulations on social communication, ethics, social peace, promoting the idea of human rights, protecting the dignity, especially children and youth in the media, etc.

It is consulted before any contentious appeal concerning refusal or withdrawal of the press card. It has disciplinary powers towards bodies and professionals of the social communication sector. The disciplinary measures are warning, temporary suspension of activities, definite ban of activities.

REPRESSIVE MEASURES

They include the putting in place of judicial institutions as well as sanctions for the violation of the right to privacy in the electronic communication sector.

Judicial Measures

As far as judicial measures are concerned, Cameroon laws provides for penal sanctions in case of infringement of an individual's right to privacy in the electronic communications sector. This means that the violation of the right to privacy is a criminal offense punishable with loss of liberty, a fine or both. Cameroon laws give the opportunity to individuals to seek remedies for the violation of their right to privacy in the electronic communication sector through various institutions put in place to ensure that the violation of a fundamental right is remedied.

National Institutions

Several judicial institutions have been setup by the 2006 Law[xlvi]on Judicial Organisation. By virtue of article 3 of this law, the judicial organisation in Cameroon comprises the Supreme Court, the Courts of Appeal, the Special Criminal Court, lower courts in matters concerning administrative litigations, Lower Audit Courts, Military Courts, the High Courts, the Courts of First Instance and Customary Courts.[xlvii]Judicial institutions ensure that the violation of a right is punished according to the rules laid down by law. As far as the right to privacy in the electronic communications sector is concerned, the competent courts are the Courts of original jurisdictions, that is the Courts of First Instance established in each sub-division and the High Courts established in each division. Decisions of these courts can be appealed against in the courts of appellate jurisdiction which are the Courts of Appeal established in each region and the Supreme Court situated in the political Capital. Due to the fact that the violation of the right to privacy is a criminal offense in Cameroon, the said courts must sit in criminal matters. It is important to note that in matters concerning violations of the right to privacy in electronic communications sector, the legal instruments have laid down a number of penal sanctions.

In accordance with the provisions of the Cameroon criminal procedure code, any victim of the violation of the right to privacy will have to seize the criminal section of either the court of first instance, or the high court, depending on whether the matter is a felony of a misdemeanor. That notwithstanding, an individual can equally claim damages for such violation. In case the victim is not satisfied with the decisions of the national institutions, it can seize the international institutions.

The procedure to be followed in case of violation of the right to privacy in the electronic communication sector is that laid down in the Cameroon Criminal Procedure Code. However, the Law on Cyber Security and Cyber Criminality lays down some procedures to complement that of the Criminal Procedure code.[xlviii] It states that investigations may be done by Criminal Investigation officers, such as the Judicial Police, as well as officials of the NAICT.[xlix] They may visit the *locus in quo* in order to carry out searches and proceed to seizures with the aim of gathering evidence to prove the violation of the right to privacy.[l]

For security purposes, when a copy of data is seized, the State Counsel may order its destruction. Only objects, documents and data used as evidence may be kept under seal and this must be authorized by the State Counsel. If the data or information has been transformed or modified, the State Counsel, examining magistrate or Court may request that a clearer version of the data be obtained. This can only be done by experts such as qualified natural persons or companies having the technical capacity to do so.

Equally, if one the violators of the right to privacy resides in a different territory than where the investigation is being carried out, a rogatory commission may be setup be it at the national or international level to search the elements of the crime or the perpetrators of this right.[li] This commission shall perform its duties in accordance with the provisions of the Cameroon Criminal Procedure Code and Subject to rules of reciprocity between Cameroon and foreign countries with which it has concluded a judicial cooperation agreement.[lii] The aim of this commission is to ensure that whoever violates the right to privacy does not go unpunished by escaping into a different territory or country.

International Institutions- The African Court and The Commission on Human and Peoples Rights

The African Court on Human and Peoples' Rights is a judicial body that delivers binding judgments on compliance with the African Charter. It renders provisional and final judgements in accordance with the Protocol establishing the said Court. In case of any violation of an individual's right to privacy in electronic communication sector in Cameroon, the Court can order compensation or reparation of the wrong done. This is due to the fact that Cameroon ratified the Charter on July 23, 1987.

An individual whose right to privacy has been violated can apply directly to the Court or can pass through the African Commission or other intergovernmental organisations as well as the Government of his country. However, for his/her matter to be admissible, the individual must have exhausted the local remedies and must show proof of exhaustion of these local remedies.[liii]The written application must be filed at the seat of the Court which is in Arusha-Tanzania.[liv]. It must be signed by the individual or his representative. It must state all the details

concerning the applicant as well as the respondent and must equally indicate the alleged violations and order sought. However, there is no time limit required for an individual to file his application before the Court.[lv] Under article 46 of the Charter, the Commission has the power to use any appropriate method of investigation into allegations of human rights abuses.[lvi] Where the Commission finds that violations have occurred, it makes recommendations to to ensure that the occurrences are investigated, that the victim whose right to privacy has been violated is compensated and that measures are taken to prevent the recurrence of the violations.[lvii]

It is important to note that though the right to privacy has not explicitly been stated in the African Charter, article 3 of the Protocol to the African Charter on Human and Peoples' Rights on the Establishment of an African Court on Human and Peoples' Rights, June 10, 1998 gives the court the mandate to consider violations under any relevant human rights instruments as ratified by Cameroon.

Specific Actions Constituting Violation of The Right to Privacy In The Cameroon Electronic Communication Sector And Their Corresponding Penalties

Cameroon legislator has put in place a number of repressive measures to deter the violation of the right to privacy in Cameroon. Some of these measures could be seen in the Penal Code, the Law on Cybersecurity and Cyber Criminality, the 2010 law on electronic communications. Some of these acts are felonies while others are misdemeanors.

Felonies

As far as privacy is concerned, the main act that constitutes a felony is unauthorized access to electronic communication network or system. Due to the confidentiality of communication in the electronic communication sector, the law punishes any one whom without authorization proceeds to access all or part of an electronic communication network or an information system or a terminal device and violates the integrity, confidentiality, availability of the electronic communication network or the information system. Such individual shall punish with

imprisonment for from 10 (ten) to 20 (twenty) years or a fine of from 10.000.000 (ten million) to 20.000.000 (twenty million) CFA francs or both such fine and imprisonment.[lviii]

Misdemeanors: Violation of the secrecy of a correspondence

Confidentiality of communications and correspondence is a rationale for the protection of the right to privacy in the electronic communication sector. Since electronic communications are an important means of expressing private thoughts and feelings and developing relationships with others, monitoring, intercepting listening, reading or divulging people's communications will often involve infringing their right to privacy. Consequently, the right to correspondence confidentiality or secrecy provides a barrier against unwanted access to these private thoughts, feelings and exchanges, and thereby protects individual privacy.[lix] In this light, when called to participate in the execution of an electronic communication service, any person who violates the secrecy of a correspondence or who without authorization divulges, publishes or uses the content of such correspondence without the authorization of the author shall be punished with imprisonment of from six (06) months to two (02) years and a fine of from 1.000.000 (one million) to 5.000.000 (five millions) or both such imprisonment and fine.[lx] Likewise any person who intercepts a private conversation either voluntarily or involuntarily and goes ahead to discloses same.[lxi]

Equally, any person who fraudulently or without authorization becomes acquainted with, delays access to or deletes electronic messages addressed to another, intercepts, diverts, uses or divulges electronic messages sent or received by electronic means or proceeds to install equipment designed for such interceptions 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.[lxii]

However, these sanctions will not be applicable if these people obtain an authorization from author or recipient of the private conversation. Equally, sanctions will not be applicable if this interception is requested by a judicial authority, or during control necessary for technical reasons, or when such interception is necessary for service provision and verification of the quality of services and is necessary for the protection of rights directly linked to the provision of electronic communication. As such, though the law puts in place severe measures to punish

those who infringe the right to a person's privacy through the violation of his right to have a secret correspondence, it at the same time lays down limitations to such punishment.

Unauthorized reception, interception, collection and processing of the privacy of another

Cameroonian laws punish anyone who 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. If any person carries out such act, he/she 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.[lxiii] If someone intercepts personal data in the course of their transmission, from one information system to another without authorization, he/she shall face the same punishment.

More to that, the law on cyber security and cyber criminality punishes any person who, even though negligence processes or causes the processing of personal data in violation of the conditions precedent to their implementation 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.[lxiv]

Again, anyone who 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. If such data is disclosed, the person who discloses such information 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 50 000 000 (fifty million) CFA francs or both of such fine and imprisonment. [lxv] Equally, 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, he/she shall be punished with imprisonment of from 1 (one) year to 04 (four) years or a fine of from 2 000,000 (two million) to 10,000,000 (ten million) CFA francs or both of such fine and

imprisonment. This goes in line with the fact an individual is the only person who decides on what he wants people to know about him.

Recording or publishing of images undermining the bodily integrity of an individual

The provisions of Cameroonian laws are to the effect that any individual who for financial gain, records or publishes images that undermine the bodily integrity of another person through electronic communications 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. However, the law states an exception to this which is the fact that no one shall be punished if 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.[lxvi]

Indecency towards an individual

The law is to the effect that in situations where someone has been put in contact with another person using an electronic communication system and the latter commits private acts of indecency towards the former without his consent and notwithstanding whether it is open to public or not,[lxvii] he/she 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.[lxviii]

Actions constituting violation of children's privacy

As far as Children's right to privacy is concerned, the law lays down provisions to punish those who violate this right in the electronic communication sector.

Its provisions are to the effect that 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.[lxix]

Equally, the law punishes those who for consideration or free of charge, use electronic communications or an information system to publish, import or export, attach, record or transmit an image or picture showing or portraying 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.[lxx]

Those who keep an image or picture portraying pedophilia in an electronic communication network or an information system shall equally 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. This penalty shall be doubled where an electronic communication network is used to publish an image or picture of a minor.

In a nut shell, it can be seen that Cameroonian law recognizes and protects the right to privacy in the electronic communication sector. It lays down acts which can be considered as those in violation of the right to privacy and puts into place measures and procedures to be followed to remedy acts constituting violation of the right to privacy. That notwithstanding, Cameroonian laws authorize violation of the right to privacy in very limited circumstances and by a certain category of people and for specific purposes. So, the Cameroon government ensures the realization of the right to privacy in its electronic communication sector though such realization is limited.

ENDNOTES

[i] Fried, C., '*Privacy*', The Yale Law Journal Vol. 77, No. 3. (1968) p. 482.
[ii] Westin, A. F., '*Social and political dimensions of privacy*' Journal of Social Issues Vol 59, No. 2. (2003). p. 431.
[iii] Hajdú J.: *A munkavállalók személyiségi jogainak védelme*. Pólay Elemér Alapítvány, Szeged, (2005). p.8.
[iv] Louis Brandeis and Samuel Warren, *'The Right to Privacy'* Harvard Law Review. (1890). pp. 193-220.
[v] United Nations General Assembly, International Convention on the Protection of Migrant Workers and Members of their Families adopted by the resolution 45/158, (18 December 1990).
[vi] Convention on the rights of the child adopted by the United Nations General Assembly resolution 44/25, (20 November 1989 and entered into force on 2 september1990).
[vii] African Charter on the Rights and Welfare of a Child Adopted by the Organisation of the African Unity in (1990 and entered into force in 1999).
[viii] African Charter on Human and Peoples' Rights which Cameron ratified on (23 July 1987).

[ix] Directive No 07/08-UEAC-133-CM-18 laying down the legal framework for the protection of the rights of users of the electronic communication services in the CEMAC region of 19 December 2008.
[x] Law N° 2008/001 of 14 April 2008 to amend and supplement some provisions of law N° 96/6 of 18 January 1996 to amend the Constitution of 2 June 1972.
[xi] Articles 41 to 48 of law n° 2010/012 of 21 December 2010 relating to cybersecurity and cyber criminality in Cameroon.
[xii]Article 4.
[xiii] No 2010/013 of 21 December 2010 governing electronic Communications in Cameroon and its amendment of April 2015.
[xiv] Article 4.
[xv] *Ibid*, article 5 point 15.
[xvi] *Ibid.*
[xvii] Article 43 of n° 2010/012 of 21 December 2010 relating to cybersecurity and cyber criminality in Cameroon, number 6 above.
[xviii] Directive No 07/08-UEAC-133-CM-18 laying down the legal framework for the protection of the rights of users of the electronic communication services in the CEMAC region of 19 December 2008, number 9 above.
[xix] Article 3.
[xx] Article 80.
[xxi] Article 5.
[xxii] *Ibid*, articles 60 to 85.
[xxiii] Global Internet Liberty Campaign, 'Privacy and Human Rights- An international survey of privacy Laws and Practice' available at https://www.gilc.nl/privacy/survey/intro.html, [accessed on June 11, 2020].
[xxiv] Office of the United Nations High Commissioner for Human Rights and World Health Organisation, 'The Right to Health' Fact Sheet No. 31, (2008), pp.25-26.
[xxv] *Ibid.*
[xxvi] *Ibidem.*
[xxvii] Peter Sagal, 'Privacy & Property Rights' available at https://www.pbs.org/tpt/constitution-usa-peter-sagal/rights/privacy-and-property-rights/, (retrieved on 12 May 2020).
[xxviii] Article 41 of law n° 2010/012 of 21 December 2010 relating to cybersecurity and cyber criminality in Cameroon.
[xxix] *Ibid*, articles 41 to 48.
[xxx] Article 46.
[xxxi] Article 49.
[xxxii] Article 54 of Law No 2010/013 of 21 December 2010 regulating electronic communications in Cameroon, as amended by law No 2015/006 of 20 April 2015.
[xxxiii] Article 33 and 34 of the 2010 Law on Cybersecurity and Cyber Criminality.
[xxxiv] *Ibid.*
[xxxv] Article 43.
[xxxvi] Article 46(2)
[xxxvii] Article 44.
[xxxviii] Article 48
[xxxix] *Ibid.* Article 35.
[xl] Article 7 of Decree No 2013/0399/PM of 27 February 2013 laying the modalities for the protection of Consumers Protection in the electronic communication network in Cameroon.
[xli] *Ibid*, article 8.
[xlii] Decree No 2012/180, of 10 April 2012 on the organisation and functioning of the National Agency for Information and Communications Technology.
[xliii] Section 7 of the 2010 Law on Cybersecurity.
[xliv] National Agency for Information and Communication Technology, *'Privacy Policy',* available at https://www.antic.cm/index.php/en, retrieved on October 10, 2020.
[xlv] *Ibid.*
[xlvi] Law No 2006/15 of December 29, 2006 on judicial organisation, amended by law No 2011/027 of 14 December 2011.

[xlvii] For the composition and functioning of these courts, see articles 13 to 31 of the 2006 law on judicial organisation, amended by the 2011 law, as well as Law No 2006/016o of 29 December 2006 on the organisation and functioning of the Supreme Court.
[xlviii] Section 52 of the law on Cyber security and cyber criminality.
[xlix] Section 74 of the law on electronic communications
[l] Sections 53 to 54.
[li] Section 55.
[lii] Section 56.
[liii] Rule 34 of the African Court.
[liv] Articles 24 and 25 of the Protocol E Articles 24 and 25 of the Protocol Articles 24 and 25 of the Protocol Articles 24 and 25 of the Protocol establishing the African Court.
[lv]African Commission on Human and Peoples' Rights, available at http://www.achpr.org/fr/, (accessed on 11 May 2019).
[lvi]*Ibid.*
[lvii]*Ibid.*
[lviii] 2010 Law on Cyber Security and Cyber Criminality in Cameroon, Section 65.
[lix] Frederik J. Zuiderveen Borgesius& Wilfred Steenbruggen, 'The Right to Communications Confidentiality in Europe: Protecting Privacy, Freedom of Expression, and Trust' Theoretical Inquiries in law, Vol. 19 issue 2 (2019), pp. 291-298.
[lx] Article 80 of the law on electronic communication.
[lxi] *Ibid.*
[lxii] Section 74 of the law on Cyber security and Cyber criminality.
[lxiii] Section 74. (1)
[lxiv] Section 74. (3)
[lxv] Section 74.
[lxvi] Section 75.
[lxvii] Section 295 of the Penal Code and 79 of the law on cyber security and cyber criminality.
[lxviii] Section 84 .
[lxix] Section 76.
[lxx] Section 80.