TITRE I : DROIT DES TIC (DROIT ORIENTE VERS LES TECHNOLOGIES DE L'INFORMATION ET LA COMMUNICATION).

OBJECTIFS :

Appréhender les enjeux humains et sociaux liés au développement des technologies de l'information et de la communication c'est-à-dire cerner l'impact de la manipulation des TIC sur la société et sur l'homme.

Contenu

Les thèmes suivants seront notamment être abordés :

- La protection des personnes (données personnelles automatisées, fichiers, libertés, protection des mineurs) ;
- La protection des consommateurs (jeux, ventes à distances) ;
- La sécurité des systèmes et des données (cryptologie, mot de passe, code, signature électronique, licence…) ;
- La protection des créations intellectuelles : logiciels, bases de données, produits multimédias) ;
- Aspects contractuels des TIC (obligations particulières s'imposant aux informaticiens, les principaux types de contrats, les prestations informatiques, licence, FAI, maintenance, infogérance…)
- Cyber droit (liberté d'expression et ses limites, les aspects internationaux du droit de l'internet, le commerce électronique, la responsabilité des Opérateurs de télécommunication (FAI, hébergeurs)

THEMES DES EXPOSES :

Il s'agit ici compte tenu du temps qui nous est imparti de travailler sur les thèmes qui ne seront pas aborder dans le cours.

Pour tout thème faire une comparaison entre le droit camerounais et le droit étranger, illustré par des cas.

1. LE FAUX ET LA FRAUDE EN INFORMATIQUE

OBJECTIFS :

 Faire ressortir la différence quant à l'objet et la différence quant aux effets

 Les mesures juridiques de lutte contre le faux et la fraude en informatique

2. LES DONNEES NOMINATIVES

OBJECTIFS :

 Faire ressortir les différents droits des individus par rapport au traitement de leurs données.

 La collecte et la détention des données nominatives peuvent telles se faire à l'insu de la personne ?

 Les dispositions légales et données nominatives

3. LES VIRUS INFORMATIQUES

OJECTIFS :

 Définition de la notion de virus informatique

 Faire ressortir les moyens de lutte contre les virus informatique

 Les dispositions légales et virus informatiques

4. - LES SIGNATURES ELECTRONIQUE ET MANUSCRITE

OBJECTIFS :

 Faire une comparaison

 Dire si la signature électronique une valeur de preuve autant que la signature manuscrite

5. - LE COMMERCE ELECTRONIQUE

OBJECTIF :

 Faire ressortir les incidences économiques et sociales du commerce électronique.

 La pratique du commerce électronique

 La loi et le commerce électronique

6. LE CYBERDROIT

OBJECTIFS :

 Faire ressortir les aspects internationaux du droit de l'internet.

 L'aspect légal du cyber espace

7. INFORMATIQUE, FICHIERS ET LIBERTES

OBJECTIF :

 Dire s'il existe un vide juridique dans la création des fichiers informatiques.

 Parler nous des libertés dans l'usage de l'informatique

 Dispositions légales concernant l'informatique, les fichiers et les libertés

8. PROTECTION DES CREATIONS INTELLECTUELLES

OBJECTIFS :

 La protection de la propriété intellectuelle dans la société de l'information

 Les dispositions entourant la protection des créations intellectuelles

9. TIC ET E-ACTIVITIES

OBJECTIFS :

 Lister les catégories des e-activities

CHAPITRE 1 : LA SOCIETE DE L'INFORMATION

INTRODUCTION

Au fil de l'histoire les technologies ont fait évoluer l'organisation de nos sociétés car elles ont ouvert la voie à des modèles de société plus durables et sont applicables dans divers secteurs.

La notion de développement durable est la finalité de l'usage des TIC principal élément utilisé dans un SI car il s'agit d'une approche globale de gestion des ressources naturelles dont le but est de satisfaire aux besoins et aspirations de l'être humain. Le système d'information est un dispositif isolé ou groupe de dispositifs interconnectés ou apparentés, assurant par lui-même ou par plusieurs de ses éléments, conformément à un programme, un traitement automatisé de données le SI est aussi entendu comme l'ensemble des éléments participant à la gestion, au stockage (l'enregistrement), traitement, transport et à la diffusion de l'information.

I- Les besoins dans les sociétés informatisées (cas de l'Afrique).

La société de l'information qualifiée de société de la connaissance désigne une société dans laquelle les technologies joue un rôle central.

Au niveau de l'Afrique il se pose un problème celui de savoir comment accéder et utiliser l'outil informatique en Afrique sans entraver les droits et les libertés des personnes?

Afin d'élaborer les stratégies de développement d'une société africaine informatisée, les actions à entreprendre sont les suivantes:

- Promouvoir l'utilisation des TIC afin d'améliorer le rendement dans la société en outre, l'utilisateur doit s'avoir exploiter l'information pour son bien être ;
- La production et l'utilisation de logiciels doit être encouragé y compris par les pouvoirs publics ;

- Les infrastructures des TIC doivent être accessibles en Afrique car le coût élevé du matériel et des licences, logiciels constituent un ensemble d'obstacles majeurs ;
- Les dirigeants doivent permettre aux bénéficiaires de comprendre parfaitement les enjeux, les ressorts et les outils ;
- Sensibilisation, vulgarisation, formation ;
- Désenclavement des zones reculées, des routes ;
- Les étudiants africains doivent avoir accès aux réseaux d'information à travers les bibliothèques électroniques ;
- L'élaboration des textes, lois et règlement par les les autorités compétentes liées à l'usage des TIC ;
- Inciter les opérateurs de télécommunications et les consommateurs à dénoncer les pratiques et les comportements illicites liés à l'usage des TIC;
- La convergence des systèmes économique, politique, culturels en ratifiant les accords internationaux d'échanges en éliminant totalement les droits de douane.
- les Africains pourront ainsi se doter des capacités nécessaires afin d'accéder à l'ère nouvelle appelée âge de l'information, l'âge de la connaissance.

II- INFORMATIQUE ET SECTEURS LIES AU DEVELOPPEMENT DANS LA SOCIETE DE L'INFORMATION

L'informatique peut être vue comme un outil au profit de la performance. Cette dernière est présente dans la quasi-totalité des secteurs (banque, assurances, industrie, services,
environnement, économe, territoires, éducation, formation, web 2.0(désigne l'ensemble des technologies et des usages du world wibe web car à la différence du web 1.0 où la plupart des contenus étaient fournis par les professionnels de

l’Internet(FAI, annonceurs, marques), le web 2.0 se caractérise principalement par la prise de pouvoir des internautes), mais se présente généralement selon trois domaines d'application distincts : L'informatique industrielle, scientifique et technologique ; L'informatique de gestion ; Les télécommunications et réseaux.

 Informatique industrielle, scientifique et technologique

L'informatique industrielle débute de l'étude de faisabilité (conception assistée par ordinateur autocad) à la production, elle concerne l'utilisation de l'outil informatique pour la fabrication de produits industriels.

L'informatique technologique concerne les applications insérées dans les appareils électroniques tels que les téléphones portables, les appareils hi-fi, les GPS (Géo Positionnement par Satellite), etc.

Quant à l'informatique scientifique elle concerne l'informatique appliquée aux laboratoires de recherche ou dans les services R&D (recherche et développement). Essentiellement basée sur l'utilisation des mathématiques, elle consiste à utiliser l'informatique pour modéliser, simuler et analyser des phénomènes.

 Informatique de gestion

L'informatique de gestion caractérise l'utilisation de l'outil informatique pour simplifier par exemple la gestion dans une administration, le suivi des clients jusqu'à la fiche de paye de l'employé (facturation, comptabilité), le suivi des étudiants en formation. L'informatique de gestion est étroitement liée au système d'information car elle permet la gestion efficace d’une société de l’information.

 Télécommunications et réseaux

Le domaine des télécommunications et réseaux désigne l'utilisation de l'informatique pour la transmission d'information et représente un vaste secteur couvrant notamment les réseaux informatiques, la téléphonie mobile ou fixe ou la télévision numérique.

III- APPLICATION DES DROITS DANS UNE SOCIETE DE L'INFORMATION

Une protection de l'individu contre la mauvaise utilisation des technologies est nécessaire et doit être prise en considération par les règlementations. L'objectif de toute régulation est en général un fonctionnement correct pour permettre le respect des valeurs supérieures de la société et assurer un minimum d'équité, faut il rappeller cette belle expression du philosophe
la cardère (19esiècle) « entre le faible et le fort c'est la loi qui libère ». la préoccupation essentielle du droit est à la fois de prohiber certains comportement et de maintenir certaines valeurs. Le droit, devant savoir s'adapter aux technologies, la Loi française n° 78/17 du 06 janvier 1978, relative à l'informatique, aux fichiers et aux libertés, L'article 23 du Statut
Général de la Fonction Publique camerounaise et les services publics, reconnaissent que tout citoyen dispose de sept droits relatifs aux traitement de leurs données dans la société de l'information il s'agit du droit d'accès direct, du droit d'accès indirect, du droit de curiosité, du droit de rectification, du droit à l'oubli, du droit à l'information préalable, du droit d'opposition. L'application des droits ci-dessus cités est importante pour le développement d'une société de l'information et leur interprétation consistera à assurer l'application et le respect des principes fondamentaux des droits de l'homme comme l'égalité et la non discrimination celà implique de mettre l'accent sur le droit au respect de la vie privée (opinion ou activités politique, religieuse, philosophique, syndicales considérée comme sensible et devant être protégé), le droit des hommes et des femmes au bénéfice égal dans les secteurs économique, socio-culturels, le droit à la liberté d'expression c'est –à-dire à ne pas être inquiété pour ses opinions, le droit à un procès équitable c'est-à-dire au respect de la présomption d'innocence et à l'égalité de tous devant la loi, du droit de bénéficier des intérêts moraux (droit d'auteur (patrimonial, moral).

CONCLUSION

Nous retiendrons que le principe fondateur de la société de l'information est le partage le plus large possible de la connaissance, de la solidarité ainsi que du progrès collectif. La société de l'information est une combinaison de la notion d'information qui est un bien public, de la communication qui est un processus de participation et d'interaction, des technologies considérées comme support d'ou l'acquisition de la connaissance principal qualificatif de la société de l'information.

CHAPITRE II: ATTEINTES ET PROTECTIONS DU SYSTEME AUTOMATISE DE DONNEES.

INTRODUCTION

Aujourd'hui, on dépend de plus en plus des systèmes automatisés pour exécuter des fonctions quotidiennes. Pour ce faire les personnes chargées de l'usage devrait en connaitre les faiblesses et prendre les mesures de sécurité qui s'imposent. Par conséquent il sera irréaliste de viser la sécurité absolue car un adversaire motivé et ingénieux qui dispose des ressources suffisantes peut compromettre la sécurité des systèmes même les plus perfectionnés.

I. QUELQUES TECHNIQUES D'ATTEINTES LES PLUS REPANDUES

a. Piratage informatique : c'est l'introduction dans un système afin de prendre connaissance, de modifier ou de détruire les données sans la permission du propriétaire ;

Quelques formes de piratage

- Le hameçonnage (phishing) : cette technique est utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but d'usurper une identité.

Elle consiste à imiter un courrier officiel, une page d'accueil d'une banque en ligne ou des clients croyants être connecté à leurs agences tapent en toute confiance leurs identifiants et mots de passe, le pirate peut en suite s'en servir pour contacter des crédits, effectuer des virements ou prendre des abonnements téléphoniques.

- Le pharming ou dévoiement: technique de piratage informatique visant à escroquer en redirigeant les internautes vers de faux sites malgré la saisie d'une

URL (adresse) valide ;

- Le harponnage ou spear-phishing : technique consistant à se faire passer pour un collègue ou un employeur afin de récupérer ses identifiants pour pouvoir accéder au système informatique de l'entreprise ;
- Hacking : c'est le faite de s'introduire dans un système informatique sans autorisation et de s'y maintenir avec une intention frauduleuse oui dans le but de nuire ;
- Smishning : Ce nouveau type d'attaque cible les téléphones cellulaires (smartphones) comme le BlackBerry.

Les propriétaires de téléphone portable reçoivent un courriel ou un SMS (Short Message Service) les incitant à suivre un lien qui installe secrètement un cheval de Troie pour les épier ;

b- Sabotage du matériel : destruction, vol du matériel ;

c- Virus : programme destiné à perturber le fonctionnement du système ou pire, à modifier, corrompre, voir détruire les données qui y sont stockées ;

d- Manipulations diverses : il s'agit ici de modifier les caractéristiques du système (panneau de configuration) à l'aide d'un droit d'accès (réorganiser les icônes, la police, l'arrière plan, son, le volume) ;

e- Décryptage : opération inverse du cryptage qui est l'utilisation de codes ou signaux non usuels permettant la conservation des informations à transmettre en des signaux incompréhensibles par des tiers.

II. RESPONSABILITE CIVILE ET PENALE

Sur le plan juridique la difficulté réside sur l'administration de la preuve d'autant plus si l'atteinte a été faite à partir d'un réseau ouvert tel que internet, l'identification de la personne peut s'avérer difficile bien que l'origine de l'atteinte est détectée, l'étendue des dommages causés à un Système automatisé,

à une entreprise ou à un utilisateur impose que des mesures de précautions soit prises

Toutefois dans un Etat de droit, la société et les individus qui la composent disposent toujours lorsqu'il y a une atteinte à leur Biens ou à leur personnes d'une alternative entre la voix pénale et la civile pour obtenir une condamnation du coupable et éventuelle réparation.

a) La responsabilité pénale.

Le droit pénal, défend l'ordre social et expose celui qui a commis un acte frauduleux à une peine ou à une mesure de sûreté.

Considérons l'infraction comme :

- Une contravention (infraction sanctionnée par une amende) Tribunal de police à compétence en ces cas
- Un délit (infraction passible de peine correctionnelle encouru par des personnes physiques (emprisonnement, amende, sanction réparation) le tribunal Correctionnel composé d'un magistrat professionnel) à compétence en ces cas
- Un crime (homicide, action blâmable) la cour d'assise composé d'un jury populaire.

b) La Responsabilité civile.

Le droit civil a un caractère strictement compensatoire puis qu'il régisse des dommages et intérêts et organise la réparation des préjudices subis par les individus.

Le principe général de la responsabilité civile est exposé par l'article 1382 du code civil «Tout fait quelconque de l'homme qui cause à autrui un dommage oblige celui par la faute duquel il est arrivé à le réparer. » et 1383 « chacun est responsable du dommage qu'il à causé non seulement par son fait mais encore par

sa négligence ou son imprudence. » La responsabilité civile de toute personne peut être engagée si trois (3) conditions sont remplies :

- Un préjudice subi par la victime.
- Une faute de l'auteur du délit.
- Un lien de causalité entre le préjudice subi et la faute.

c. La compétence du lieu de commission de la faute.

Le tribunal qui sera assigné sera celui du lieu du fait dommageable.

III. LES TECHNIQUES DE SECURITE DANS UN SYSTEME D'INFORMATIQUE.

La sécurité est l'un des moyens techniques et logiciels mise en place pour conserver et garantir la bonne marche du système.

a. La protection physique.

Elle concerne la sécurité au niveau des infrastructures matérielles On s'engagera à :

- assurer la réparation des erreurs de fonctionnement (maintenance corrective) à prévenir celle-ci par des vérifications périodique c'est-à-dire voir si le matériel et le logiciel fonctionnent bien (maintenance préventive), On peut également faire une maintenance évolutive (installation et mise à jour) ;
- rechercher un endroit aéré et sec ;
- éviter la poussière ;
- respecter la démarche d'arrêt et de démarrage

b. La protection dans le système d'exploitation Windows.

Windows, rencontre beaucoup de critique sur son manque de sécurité (contrairement au SE linux) mais possède pourtant des ingrédients sûrs :

- La notion de session c'est-à-dire l'authentification de l'utilisateur qui est à la base du mécanisme de sécurité de Windows.
- Interdiction du partage des comptes (création de plusieurs comptes, désactiver les comptes inutilisés).
- Activer les fonctions essentielles de sécurité c'est-à-dire activer le pare-feu/firewall (barre de tache-alerte de sécurité Windows – protection pare-feuactiver) ou bien panneau de configuration et activer)
- La notion de sécurité dans un navigateur à l'exemple d'internet explorer (outiloption internet-paramétrer les options de sécurité (sécurité avancé…)

c. La protection logique.

- L'installation des programmes antivirus :

Les antivirus, sont des programmes permettant de détecter et de localiser la présence d'un virus, afin de tenter de réparer les fichiers endommagés, de les mettre en quarantaine ou de supprimer les fichiers contaminés.

Bien qu'elle ne vous mette pas à l'abri de tout danger, la meilleure protection consiste à installer sur l'ordinateur un logiciel antivirus. Cependant de nouveaux virus apparaissent chaque jour, Il importe donc d'installer des logiciels compatibles et d'actualiser régulièrement le logiciel.

- Activer un filtre anti spam :

Les spam ce sont des informations à caractère publique qui engorge nos boîtes aux lettres. Le filtre anti-spam sert à identifier les mails caractérisés de spam. Dès lors, ils n'arrivent pas jusqu'à votre boîte électronique.

- Installer un pare-feu : considéré comme un administrateur système (dispositif logiciel et matériel qui filtre le flux de donnée sur un réseau informatique) il

permet de protéger un ordinateur dans un réseau tiers (exemple internet) en filtrant des données échangées dans le réseau, d'empêcher les attaques des antivirus nuisibles, de bloquer une prise en main à distance par un pirate.

- Installer un antispyware :

Le spyware est un logiciel malveillant qui s'installe dans un ordinateur dans le but de collecter et de transférer des informations très souvent sans que l'utilisateur n'en est connaissance. Un anti-spyware est une famille de logiciels destinés à éparer et à supprimer les spywares qui pullulent sous Windows Exemple : AVG (anti-spyware).

- Le cryptage des données ou cryptologie :

Le cryptage est un procédé grâce auquel on peut rendre la compréhension d'un document impossible à toute personne qui n'à pas la clef de déchiffrement. Le cryptage garantit la confidentialité des données (en chiffrant ou en déchiffrant) à l'aide des logiciels basés sur des algorithmes.

CONCLUSION.

Il serait naïf pour tout utilisateur de se croire à labri des introductions non autorisées dans un système informatique sous prétexte son ordinateur ne contient rien d'extraordinaire.

Par les méthodes de sécurités, l'on peut se préserver de l'introduction, la fraude, de la modification ou l'effacement de données. En cas de faute commisse, l'auteur sera puni ou tenu de réparer le tort, néanmoins pour échapper aux poursuites judicaires le présumé auteur pourra tenter d'évoquer sa bonne foie en faisant valoir qu'il ignorait l'interdiction.

CHAPITRE III : INFORMATIQUE, LIBERTES et DROITS DES INDIVIDUS.

INTRODUCTION

Les TIC offrent beaucoup de commodité dans le travail. Parmi les nombreux avantages, on peut citer : la mise à la disposition des usagers aux sources d'informations. (Internet à partir de moteurs de recherche). L'accès rapide à l'information. Les correspondances rapides. Cependant, elles n'ont pas que les avantages elles peuvent faciliter la tâche à des personnes mal intentionnées pour porter atteinte aux mœurs. La mésaventure est arrivée à une jeune fille filmée nue par son copain, les images ayant été rendues publique, outré de voir son intimité faire le tour de la ville elle a porté plainte contre son copain qui a été jugé coupable d'attentat à la pudeur.

Il importe d'être sensibilisé au contexte entourant la circulation de l'information dans l'utilisation des TIC à cet effet, l'élaboration d'une structure de surveillance sur Internet, la détection de crimes commis dans des environnements virtuels, l'amélioration des outils de recherche de renseignements face aux problématiques émergentes et la veille technologique constituent des moyens possibles pour y faire face.

I. LES INFORMATIONS NOMINATIVES

Par informations nominatives on entend toutes informations qui permettent d'identifier un individu directement (Nom, Prénom…….) ou indirectement (numéro de téléphone, adresse email) .sachant que chacun à droit au respect de sa vie privée, le problème qui se pose est de savoir quelles sont les droits que détiennent des personnes fichées ? (Les personnes fichées doivent-elles être informées sur les droits dont elles disposent face au traitement automatique de

leurs données ? Qu'est-ce qu'on cherche à protéger ?) Pour répondre à cette question, on se basera sur l'individu car il constitue l'objet de la protection.

La protection des données nominatives est une forme de reconnaissance des personnes comme être libre ainsi la collecte et la détention des données ne peuvent se faire à l'insu de la personne car elle dispose d'un droit d'accès et de rectification.

L'information nominative est aussi entendue comme une information qui concerne une personne physique particulière, telle qu'un dossier médical, un relevé de notes d'un étudiant ou un casier judiciaire. Pour obtenir ce type d'information, le droit exige du requérant qu'il ait un intérêt pour («être concerné par») le document nominatif auquel il souhaite accéder. La loi française de 1978 mentionne la nécessité de protéger la vie privée de la personne fichée. (En application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, chaque membre dispose des droits d'opposition (art. 26 de la loi), d'accès (art. 34 à 38 de la loi) et de rectification (art. 36 de la loi) des données le concernant.)

Une étude camerounaise a établi la distinction entre le droit d'accès à l'information et le droit à la liberté d'expression.

Il ressort de cette étude que, même si le Cameroun ne dispose pas d'une loi générale d'accès à l'information, la Constitution du 18 janvier 1996 reconnaît et consacre dans son préambule la Charte Africaine des Droits de l'Homme et des Peuples et la Déclaration Universelle des Droits de l'Homme. Ainsi les droits à la liberté d'accès à l'information des articles 9 de la Charte africaine des droits de l'homme et des peuples, et 19 de la Déclaration universelle des droits de l'homme respectivement sont parties intégrantes de la législation nationale du Cameroun.

L'administration camerounaise comprend l'importance de permettre l'accès des personnes aux dossiers les concernant, de même que la nécessité de ne pas divulguer à des tiers les informations ne les concernant pas Etude de cas : Obtention de dossiers médicaux personnels dans les hôpitaux. A la question de

savoir si les malades pouvaient avoir accès à leurs dossiers, le médecin chef de l'hôpital a laissé entendre que «les dossiers médicaux sont la propriété de l'hôpital» et que s'ils veulent y avoir accès, ils doivent obtenir la permission du médecin traitant.

L'accès aux documents judiciaires constitue également un important défi pour les citoyens du fait de la longueur et du coût de la procédure y afférents. Pour les documents délivrés par les autorités judiciaires tels que le certificat de nationalité, les extraits de casier judiciaire ou les extraits de registres de commerce ou des hypothèques, la délivrance est sujette à la production d'une demande timbrée, d'un formulaire timbré et au paiement de frais d'enregistrement. Pour les documents juridictionnels (grosses, expéditions, certificats de non appel, certificats de dépôt etc.) et les documents extra juridictionnels tels que les actes d'huissier, il faut en plus des droits de timbre, procéder à l'enregistrement avant la délivrance desdits actes (articles 91 et suivants du code de l'enregistrement du timbre et de la curatelle.

Cependant, il existe une disposition spéciale pour les fonctionnaires qui souhaitent accéder à une information nominative concernant leur dossier de carrière et leur vie professionnelle. Le fonctionnaire camerounais est considéré comme un propriétaire privilégié du droit d'accès à l'information qui le concerne. L'article 23 du Statut Général de la Fonction Publique dispose que, Le fonctionnaire a le droit d'accéder à son dossier professionnel personnel et peut entre autres choses demander à l'administration la clarification, la rectification, la mise à jour, le complément ou le retrait d'une information imprécise, incomplète, équivoque ou dépassée ou alors dont la collecte, l'utilisation, la divulgation ou la conservation sont interdites. Lorsque le fonctionnaire concerné en fait la demande, l'administration compétente doit procéder, gratuitement pour le fonctionnaire, au changement sollicité.

L'information non nominative est celle qui n'est pas spécifique à une personne mais qui renvoie

Plutôt à une information qui concerne le public en général, ou les activités et fonctionnement de l'Administration. Il peut s'agir d'un document sous n'importe quelle forme, soit écrit (rapports, opinions ou décisions), sonore, visuel ou automatisé, qu'ils soient de nature factuelle ou juridique.

II. QUELQUES AGISSEMENTS ILLICITES SUR INTERNET

Un délit est un délit sur Internet ou ailleurs. Les agissements délictueux étant innombrables on peut citer :

a. la pédopornographie

La pédophilie est définie comme une préférence sexuelle pour les enfants généralement en âge pré-pubert ou au début de la puberté. La pornographie est la représentation obscène dans une œuvre littéraire ou cinématographique. Prés d'un millier d'images pornographiques représentants des mineurs sont en circulation permanente dans le réseau. Les services d'images pornographiques sont rarement situés en France ou en Europe mais plutôt aux U.S.A, en Asie, Russie…

* Illustration d'un cas.

Raymond GERMANO ,68 ans général français à la retraite a comparut mardi le 3 Novembre 2009 pour avoir téléchargé des images pornographiques mettant en scène des enfants de 6 mois à 12 ans. L'affaire remonte à l'année 2006. Des policiers autrichiens au cour d'une enquête se sont intéressés à un site Internet diffusant des images et des vidéos pornographies principalement pédophilies. L'enquête a permis de repérer les utilisateurs du site dont le général. La trace de celui-ci a été remontée grâce à l'adresse de son ordinateur.

Il n'a d'ailleurs pas nié les faits et s'est dit près à se soumettre à un traitement. Son ordinateur a été saisi près de 3000 photos ont été retrouvées dans son disque dur. Il a encouru une peine de 2 ans et une amande de 30.000 euros.

b. les copies ou reproductions d'œuvres. (Respect de la loi sur la Propriété intellectuelle)

A titre de droit comparé, l'article 335/4 du code de la propriété intellectuelle français punit de 3 ans d'emprisonnement et de 300.000 euros d'amande, toute reproduction, communication ou mise à la disposition du public à titre onéreux ou gratuit toute prestation réalisée sans l'autorisation. Au Cameroun, les reproductions des œuvres sont réglementées par la loi n° 2000/11 du 19 Décembre2000 relative aux droits d'auteur et aux droits voisins (droits développés autour du droit d'auteur : interprètes et exécutant, producteurs de phonogrammes organismes de radiodiffusion).

Dans le Cas d'utilisation de logiciels Microsoft lance la SOCILADRA aux trousses des entreprises, des personnes physiques et même des administrations publiques, celles-ci reçoivent des correspondances les prévenant de l'imminence d'une campagne engagée par la sociladra dans le but de vérifier la conformité des parcs informatique par rapport à l'utilisation des logiciels authentique. (Il est question ici de s'assurer de l'authenticité de l'usage des logiciels par les personnes physiques, les grandes entreprises et même les administrations publique.) par mesure de sureté la sociladra prévient pour toute éventuelles résistances des peines allant de 5 mois à 2 ans de prison avec des amandes allant de 500 000 à 10 000 000 FCFA à titre de dommages et intérêts.

Dans le Cas de copie privée

En mettant une copie non autorisée à la disposition de ses amis et du public l'auteur de la copie se situe manifestement en dehors du cercle de la famille et de l'usage privé du copiste et peut de ce fait être poursuivi.

c. Les menaces sur Internet.

La plus part des menaces sur le Internet ne peuvent se classer dans l'une des catégories suivantes :

- La perte de l'intégrité des données ici, les informations sont créées, modifiées ou supprimées par un intrus.
- La perte de la confidentialité des données : ici les informations sont accessibles à des personnes non autorisées.
- La perte de services : un service est défaillant en raison de l'action d'un pirate.

Exemple de menaces sur internet : diffamation, injure, menace de mort, calomnies.

 diffamation

La diffamation est une allégation qui porte atteinte à l'honneur de la personne. Les infractions commisses sur Internet sont de plus en plus nombreuses tout particulièrement du faite de la diffusion des propos diffamatoires (injurieux voire incitant à la haine raciale ou en encore à la violence)

La loi camerounaise de 1990 sur la liberté de la presse s'applique sur internet et protège les personnes et les institutions privées contre les informations et commentaires qui leur ont porté préjudice à charge pour elle d'en demander réparation.

Un webmaster quelqu'un écrit sur son site web ou sur un forum qu'un tel n'est pas journaliste et qu'il est plutôt mythomane (tendance au mensonge) si le journaliste attaque cette personne en montrant des contrats, des fiches de paye, insi qu'une carte de presse, l'affaire risque de mal tourné pour notre diffamateur surtout si le journaliste présente un certificat médical d'un psychiatre le présentant comme étant un individu sérieux et équilibré. (si l'on dispose de toute les pièces pour démontrer une diffamation : certificat, lettre de moralité, constats par huissier de justice…) l'on aura juste qu'à commencer à compter ce que nous devra la personne qui vous a diffamé en demandant aussi le remboursement des frais judicaires).

Le responsable de propos diffamatoires est souvent impossible à identifier car caché derrière son anonymat plus que protecteur, l'hébergeur afin d'éviter que sa responsabilité soit engagé il devra détenir et conserver les données d'identification de toute personne ayant contribué à la création du site litigieux.
La diffamation va dans le même sens que les menaces de mort, calomnies…

III. LA LIBERTE D'EXPRESSION ET SES LIMITES SUR INTERNET.

La liberté d'expression consiste pour n'importe qui à pouvoir faire connaître au plus grand nombre n'importe qu'elle opinion. Le problème est qu'avec la liberté d'expression, insulte, racistes, diffamations diverses, incitation au meurtre, à la violence ne manquera pas de fleurir sur la toile. En faveur de cette liberté, on peut considérer que ce n'est pas en interdisant qu'on élimine des opinions criminelles des têtes, ce n'est pas en condamnant des propos racistes ou homophobes qu'on fera reculer ces maux dans les consciences .il se pose donc le problème de savoir qui décidera si tel propos est excessif et si tel autre est acceptable.
Plusieurs types de discours sont prohibés mais pour qu'un propos soit interdit il faut identifier le danger. Certains internautes n'hésitent pas à faire héberger leurs sites vers les pays plus permissifs en matière de liberté d'expression (la Russie, le Japon, U.S.A). L'on considère qu'en Europe, les propos anti-sémites sont délictueux aux U.S.A ils sont l'expression d'une opinion.
La liberté s'accompagne des limitations des droits et de la dignité d'autrui. Les mesures visant à empêcher une atteinte à la liberté d'autrui peuvent être prescrites comme ce fut le cas en Angleterre et aux U.S.A.
En Angleterre un système de mouchard facilite les écoutes sur Internet. Ce système est mis totale se met en place pour protéger les citoyens.
Aux U.S.A après le 11 septembre 2001, le FBI a mis en place le système CARNIVORE (logiciel de surveillance installés chez les F.A.I afin de surveiller

la circulation des messages électroniques et de conserver l'historique des consultations).

IV. LA RESPONSABILITE DES OPERATEURS AU REGARD DES CONTENUS ILLICITES.

Sur Internet, celui qui subit un préjudice aura tendance à mettre en cause les opérateurs. Illustration d'un cas :

Une série de photographies privées représentant la dénommée Estelle partiellement et complètement nue était diffusées sur un site. Dans son ordonnance, le TGI (Tribunal de Grande Instance) de Paris constate qu'il a été porté atteinte aux droits d'Estelle sur son image. Il a été précisé que cette atteinte est du fait du titulaire du site mais qu'on conviendra toutes fois de s'interroger sur la responsabilité de l'hébergeur, Valentin le gestionnaire du service en tant que fournisseur d'accès et d'hébergement soutiendra qu'il ne peut être tenu responsable du contenu mis en cause. Le juge a tenu à précisé que le fournisseur d'hébergement à l'obligation de veiller à la bonne moralité de ce qu'il héberge. Le tribunal ordonna à valentin de mettre en œuvre des moyens de nature à rendre impossible toute diffusion des clichés photographique et ce sur l'astreinte de 100.000 euros/jrs.

Les hébergeurs des sites devront contrôlés à priori les pages qu'ils abritent, ces derniers ont une obligation de prudence, de vérification contenu ou du thème d'un site et les F.A.I bloquer les données constituants les infractions, Les Etats encouragent les opérations de télécommunications et les internautes à dénoncer aux autorités les délinquants ou les comportements illicites sur internet.

CONCLUSION

Bien que le pacte international au droit civil et politique protège le droit à ne pas être victime de discrimination, le droit au respect de sa vie privée, le droit à la liberté d'opinion et d'expression, l'article 10 de la convention européenne des droits de l'homme garantit la liberté d'expression et de l'informatique, la charte Africaine des droits de l'homme et des peuples garantit quant à elle dans son article 2 le droit à ne pas être victime de discrimination ; on pourrait penser à la création d'un organisme international basé sur les droits peuples admis par tous afin de lier l'informatique aux libertés et aux droits des individus principaux utilisateurs des TIC.

CHAPITRE IV : LES CONTRATS INFORMATIQUE

INTRODUCTION

Le droit des contrats est dominé par le principe de la liberté d'autonomie, de la volonté, la liberté contractuelle car chacun est libre de contracter et du choix de son contractant.

Les contrats informatiques, désignent tout accord ayant pour objet une vente, une location ou une prestation de service relative à un système d'information ou à un élément intégré, susceptible d'être intégré dans un système Un contrat n'est volontairement formé s'il réunit un certain nombre d'éléments prévus par l'article 1108 du code civil camerounais :

- La capacité de contracter.
- L'objet qui forme la matière de l'engagement.
- La cause licite.
- Le consentement doit être libre, il ne doit comporter aucun vice (l'erreur, le dol (manœuvre frauduleuse destinée à tromper), la violence)

A défaut de ces éléments, le contrat est nul.

I- LES PRINCIPAUX TYPES DE CONTRATS INFORMATIQUES

a) Licence d'utilisation

L'objet du contrat est protégé par le droit d'auteur, la distribution et l'utilisation sans licence sont interdite, c'est donc un droit d'usage de l'utilisateur sans transfert de propriété.

(Une licence exclusive étant très couteuse, un éditeur concède à un client un droit d'usage sur le logiciel dont il conserve la propriété intellectuelle.)

Le droit d'usage accordé est délimité dans le contrat et doit être dans les termes clairs et précis pour que l'utilisateur ne se retrouve pas contrefacteur en cas d'utilisation non autorisé

b) Licence d'exploitation

Ici il est conféré au licencié un droit d'utilisation et un droit d'adaptation car les programmes sources sont transmis (Logiciel libre : logiciel distribué avec l'intégralité de ses programmes sources, afin que l'ensemble des utilisateurs qui l'emploient puissent l'enrichir, le redistribuer à leur tour.

c) Contrat d'entretien et de suivi

Ce sont des contrats de maintenance, cette prestation consiste à maintenir un système informatique dans un état de fonctionnement conforme aux exigences contractuelle, le prestataire peut s'engager soit à faire une maintenance corrective, préventive ou évolutive.

d) Contrat d'aide à la décision

Permet de choisir un nouveau système en procédant à un audit, nous distinguons ici deux types de contrat.

Contrat de conseil : ici le fournisseur conseil son client dans le choix d'un matériel informatique satisfaisant ses besoins et compatible à son environnement ;

Contrat d'audit : c'est l'étude des conditions de fonctionnement d'une entreprise, il s'applique aux besoins d'un client déjà informatisé.

e) Contrat de fourniture de solution informatique

Nous distinguons ici cinq types de contrats :

Contrat de vente : ici une partie s'engage à remettre à une autre une chose moyennant un prix. Dans le cadre de la vente de matériel, le fournisseur est soumis à l'exécution d'une démonstration préalable satisfaisante, établissant la compatibilité du matériel vendu avec l'environnement de son client.

Contrat de location : ce contrat lie un bailleur et un locataire pour la mise à disposition du matériel informatique. Les clauses sont : la désignation du matériel,

la durée, les montants de la location, les conditions d'utilisation du matériel, la garantie. Le locataire est obligé de maintenir le matériel en l'état.

Contrat de crédit bail : c'est la location d'un bien assortie d'une promesse unilatérale de vente. L'un des avantages du crédit bail est de devenir propriétaire du matériel pour une infime somme à la fin de la période de location. Or dans le domaine de l'informatique caractérisé par une évolution des technologies, le client se retrouve souvent en fin de contrat en possession d'un matériel déjà dépassé.

Contrat de développement de logiciels : ici, le prestataire s'engage envers le client à réaliser un logiciel conforme à ses besoins exprimés dans un cahier des charges.

Contrat de fourniture d'une solution clef en main : le maître d'ouvrage (client) fera appel aux services d'un maître d'œuvre (spécialiste), capable de lui fournir une solution

f) Contrat d'infogérance :

L'infogérance (correspond à la prise en charge complète du système) est le fait de confier tout ou partie de ses moyens informatiques à quelqu'un qui traitera le système d'information à votre place. C'est pourquoi le terme d'externalisation est également employé. L'infogérant qui a en charge ce système d'information se substitue donc à son client pour assurer le bon fonctionnement des applications qui le composent, selon des modalités qui ont été définies et consignées dans un contrat.

g) Contrat d'hébergement de site web :

L'hébergement consiste à stocker sur le serveur (Un système d'ordinateurs qui gère et délivre des informations. IL fournit également des services à d'autres ordinateurs par l'intermédiaire d'un réseau.) d'un prestataire extérieur des pages web conçues et réalisées par l'éditeur du site en vue de les rendre disponibles vers le terminal (ordinateur ou mobile par exemple) à tout utilisateur qui en fait la demande par voie électronique.

L'hébergement est donc une prestation essentielle car, excepté dans le cas où l'entreprise dispose de ressources financières et de capacités techniques suffisantes pour devenir son propre hébergeur, elle représente le plus souvent un point de passage obligé. Ce contrat combine un ensemble de prestations qui vont permettre, via un site web, un accès ouvert ou restreint aux données mises en ligne par l'entreprise.

II- LES CLAUSES FONDAMENTALES DANS LES CONTRATS INFORMATIQUES

Les contrats sont en grande partie entourés par le droit des obligations. Pour tout contrat le prestataire est soumit a une obligation de résultat. La seule inexécution suffit à engager sa responsabilité s'il ne peut apporter la preuve d'une cause extérieure.
(Exception faite dans le cas de circonstances atténuantes, de forces majeures)
Les clauses est défini comme des engagements que doivent respecter les parties.

a) Les types de clauses

L'analyse des contrats informatiques dans leur ensemble suppose de veiller aux clauses suivantes :

- La responsabilité des co-contractants ;
- Le prix : il peut être indiqué sous forme forfaitaire ou à l'unité les conditions de payement et les pénalités doivent être prévues ; - La durée et les délais : la durée initiale du contrat est toujours indiquée, sauf si c'est un contrat à durée indéterminée. Si le contrat est à durée déterminée la reconduction peut être tacite (c'est-à-dire que le contrat est renouvelable automatiquement à son échéance sans que l'accord des signataires soit nécessaire) ou expresse (ici la volonté de renouvellement doit être exprimé par les co-contractants)

b) Les clauses abusives

Dans les contrats conclus entre consommateur ou non professionnel et un professionnel, certaines clauses sont jugées abusives lorsqu'elles ont pour objet ou pour effet de créer, au détriment du non professionnel ou du consommateur, un déséquilibre significatif entre les droits et obligations des co-contractants.

Il s'agit de la situation dans laquelle la partie forte au contrat impose sa volonté à l'autre partie. La partie faible ne peut alors qu'accepter les conditions au contrat ou ne pas contracter. Il n'existe dans ce cas aucune négociation. Le professionnel, notamment en informatique, est en position dominante. En effet, le profane ne connaît pas aussi bien l'informatique que lui et conclut un contrat dont les clauses sont abusives.

La matière étant obscure, le profane ne sait pas forcément qu'il se trouve en présence d'une clause jugée abusive. Il est donc nécessaire d'être très vigilant lorsque l'on contracte en matière informatique.

(Le professionnel est la personne physique ou morale qui contracte dans l'exercice d'une activité professionnel. Il apparaît évident que le fournisseur d'accès à Internet, l'hébergeur, le créateur de logiciel ou encore le fournisseur de matériel informatique est un professionnel.

Mais quant est-il de l'autre partie ? S'agit-il d'un consommateur/non professionnel ou d'un professionnel ? L'enjeu est important car si le cocontractant est un professionnel, la théorie des clauses abusives ne trouvera pas à s'appliquer!

Un consommateur est un profane qui n'a aucune expérience professionnelle dans le domaine où il contracte (CA Paris, 3 juillet 1998). Il conclut ce contrat de biens de consommation ou de services pour son usage personnel.

Un non professionnel est un professionnel qui conclu un contrat dans le cadre de son activité professionnelle, en dehors de sa sphère de compétence et sans rapport direct avec son activité professionnelle.

Le particulier qui contracte, par exemple, un abonnement à Internet, un hébergement de sites Web pour son usage personnel est sans nul doute considéré comme étant un consommateur.
Concernant l'entreprise qui désire s'informatiser, se connecter à Internet pour les besoins de son activité, est-elle considéré comme étant un non professionnel ou un professionnel ? La réponse est plus délicate.)

CONCLUSION

En raison de leur objet, les contrats informatiques sont complexes et appelle à une vigilance particulière lors de leur rédaction, il est nécessaire de bien définir les obligations des co-contractants et de prévoir les modalités d'interventions en cas de difficultés.
Toutefois les obligations ne peuvent pas toujours être de résultats. Les TIC n'étant pas toujours fiables à 100 % c'est l'équilibre qui permettra de nouer les relations contractuelles les plus harmonieuses possibles.

CHAPITRE IV : LES TIC ET LA PROPRIETE INTELLECTUELLE

Remarque :

Les créations intellectuelles du domaine des TIC sont incluses dans la propriété intellectuelle et ses différentes branches notons juste que c'est le mode de diffusion des œuvres qui diffère dans le système d'information.

INTRODUCTION

La propriété intellectuelle est une branche juridique qui à pour but de protéger l'esprit notamment les œuvres des inventeurs, chercheurs, producteurs, agricoles, industrielles.

Le droit de la propriété intellectuelle est justifié par la volonté de favoriser le progrès technique et l'émergence des œuvres nouvelles. Une nouvelle technologie n'est possible que grâce aux découvertes qui l'on précédée. Protéger les œuvres de l'esprit peut avoir les effets suivants :

- Stimuler la recherche en garantissant aux chercheurs la possibilité de jouir de son travail car quiconque voudra en profiter lui devra quelque chose ;
- Accélérer et spécialiser la recherche car seul le premier à déposer une invention pourra se faire reconnaître il est donc nécessaire de travailler le plus vite possible dans un domaine où le risque de se faire dépasser par un concurrent est aussi faible que possible ;

On observe une forte demande de protection dans les pays développés et une faible demande dans les pays en voie de développement considéré comme consommateur.

I- LA PROTECTION DES CREATIONS INTELLECTUELLES

L'objet de la protection du droit d'auteur est l'œuvre car elle constitue l'expression personnelle de l'intelligence et possède une originalité suffisante qui se prête à la reproduction, à la communication au public.
Les droits de la propriété sont les droits reconnus à tout auteur et lui assurant la protection des actions en contrefaçon.

A. Quelques sources de la propriété intellectuelle

- La convention de berne de 1886 pour la protection des œuvres littéraires et artistiques
- L'accord de Bangui du 02 mars 1977 révisé en 1999 relative à la concurrence déloyale et à la contrefaçon ;

La propriété intellectuelle, à pour tâche d'assurer l'enregistrement et la délivrance des titres de propriété de ces œuvres au niveau national et sous régional, L'OAPI joue ainsi un rôle important dans la naissance des droits de la propriété en Afrique;
Au niveau international L'OMPI est une institution intergouvernementale qui reçoit les demandes internationale des brevets.

B. Les œuvres du domaine du traitement de l'information

Le droit d'auteur, s'applique à toutes les œuvres de l'esprit quelque soit le genre, le format d'expression.
Dans le domaine du traitement de l'information nous aurons :

- Les bases de données sont un recueil de données ou d'autres éléments indépendant disposés de manière systématique ou méthodique et individuellement accessible par des moyens électroniques ou par tous autres moyens.

  Ici le producteur à droit d'interdire l'extraction ou la réutilisation totale ou partielle du contenu de la base de données ; pour être protégée une base de

données doit avoir nécessairement un investissement financier, matériel et humain.

- Le logiciel constitué de l'ensemble des programmes, des procédés et des règles et éventuellement de la documentation, relatifs au fonctionnement d'un ensemble de données. Le logiciel est protégé par le droit d'auteur adapté aux spécificités techniques des programmes d'ordinateur, la protection porte sur l'enchainement des instructions, le code objet et le code source, les interfaces logiques ;

Bien que la directive « logiciel » ait été votée le 24 novembre 2003 en France, l'on statuera en jurisprudence car l'intégrité des logiciels dans les œuvres protégeables par le droit d'auteur est assimilé à des œuvres littéraires et artistiques, au Cameroun, la création de logicielles constituant une solution non évidente rentre dans le domaine de la propriété littéraire et artistique selon la loi n° 2000/11 du 19 décembre 2000 ;

- Les pages web sont des compositions graphiques ou textuelles représentant des liens vers d'autres sources d'informations. Sous la condition de l'originalité, ces pages sont protégées ;
- Les sites de jeux peuvent être protégés comme des marques, les éléments esthétiques du jeu peuvent faire l'objet de dessin et modèles (propriété industrielle) ;
- Les noms de domaine sont des identifiants assignés uniquement à un site web spécifique. Il est un masque sur une adresse IP (Internet Protocole), son but est de retenir facilement l'adresse du site exemple iaicameroun est simple à retenir que 90.128.108.104. le nom de domaine et la marque ont une même force probante. Le nom de domaine est divisé en trois parties www qui indique à l'ordinateur que cette adresse est une page web, le domaine qui est le nom de domaine proprement dit l'utilisation du nom de domaine qui porte atteinte au propriétaire peut être sanctionné pour contrefaçon

II- LE DROIT D'AUTEUR A L'ERE DU NUMERIQUE

On utilise de plus en plus les techniques numériques pour créer et diffuser la connaissance. Ces techniques rendent les documents disponibles afin que les consommateurs puissent les consulter, les lire et les utiliser.

A- Le partage de ressources

Une exception au droit exclusif de l'auteur est prévue à savoir « la copie privée », cette exception marque la tolérance pour les pratique impossibles à contrôler, la plus part des copies sont utilisés dans le cadre des recherches de l'enseignement ou des études personnelles, mais l'inquiétude du titulaire des droits se manifeste sur la perte des ventes représentées par ces copies car ceux qui copient n'achètent pas forcement des œuvres.

La pratique du streaming et du peer-to-peer sont des exemples de partage des ressources

A l'aide du streaming qui est ensemble de technologies de diffusion de son ou de vidéo en flux continue sur le web un utilisateur quelconque pourra enregistrer ou télécharger n'importe quel œuvre à son profit ;

Quant au peer-to-peer c'est une technologie utilisée pour échanger les fichiers entre différents utilisateurs connectés simultanément à internet ce sont des logiciels qui mettent en ligne des œuvres protégées sans l'aval des propriétaires à destination du public, il permet également aux usagers de se les partager en toute légalité.

B- La protection technique et juridique

Plusieurs dispositifs existent pour sanctionner les comportements illicites en matière de mise à disposition d'œuvres protégées. Le piratage est facilité dans un environnement numérique d'où l'idée de protection technique des œuvres grâce au cryptage, et aux outils de filtrage permettant de déceler la circulation dans un

réseau exemple en occident, la solution COSMOS est utilisée pour permettre aux opérateurs de télécommunication d'obtenir des informations sur le comportement des utilisateurs.

Internet offre des facilités aux utilisateurs pour le téléchargement pour usage privée mais les utilisateurs sont parfois capables de contourner le système de protection technique. La protection juridique donne aux auteurs de condamner l'acte de contournement.

CONCLUSION

Durant sa vie, un auteur jouit des droit d'auteur sur sa création si elle est nouvelle, inventive te applicable à tous. Selon certains codes et organismes régissant la propriété intellectuelle, l'auteur peut par conséquent exploiter son œuvre afin d'en tirer un profit pécuniaire.

TITRE II : L'AUTORITE DE REGULATION

CHAPITRE I : L'ARTCI

L'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire (ARTCI), porte à la connaissance du public et des acteurs du secteur postal que conformément à la règlementation en vigueur, notamment la loi N°2013-702 du 10 octobre 2013 portant code des postes et ses textes d'application, le secteur postal ivoirien fait l'objet de régulation par l'ARTCI.

Il lui revient par conséquent de veiller à la mise en œuvre des dispositions du décret n°2018-382 du 04 avril 2018, fixant le montant et les modalités de paiement et de recouvrement de la contrepartie financière à la délivrance de l'autorisation de fourniture de services postaux.

Au cours de la conférence de presse tenue le 15 décembre 2020 dans les locaux de l'ARTCI, les acteurs postaux présents ont estimé que les montants des contreparties financières prévus par le décret précité sont élevés.

Les activités de livraison urbaine étant menées par une certaine catégorie d'acteurs postaux dénommés "livreurs urbains", l'ARTCI les a invités à se rapprocher de ses services à l'effet d'examiner ensemble, les dispositions pratiques visant à les accompagner dans leurs activités.

Cependant, depuis quelques jours, certaines informations circulent sur les réseaux sociaux, imputant à l'ARTCI l'intention d'écarter "les livreurs urbains" à travers des barrières financières alors qu'il n'en est rien.

L'ARTCI tient à rassurer l'ensemble des acteurs du secteur postal et la population, qu'elle exerce sa mission de régulation du secteur postal dans l'intérêt bien compris de toutes les parties prenantes et veille au bon équilibre du marché.

L'ARTCI invite à nouveau les "livreurs urbains" à prendre contact avec la Direction des Activités Postales de l'ARTCI et assure l'ensemble des opérateurs

du secteur postal de sa disponibilité à les accompagner dans le développement de leurs activités.

+++++++Une autre definition de l'artci

L'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire (ARTCI) a été créé par l'Ordonnance n°2012-293 du 21 mars 2012 à l'issue de la fusion du Conseil des Télécommunications de Côte d'Ivoire (CTCI) et de l'Agence des Télécommunications de Côte d'Ivoire (ATCI). - L'ARTCI est une autorité administrative indépendante dotée de la personnalité juridique et de l'autonomie financière.

Les missions de l'ARTCI sont déterminées par l'ordonnance n°2012-293 du 21 mars 2012 susvisée. Les missions de régulation sont exercées par l'ARTCI de façon indépendante, impartiale et transparente.

– Le siège de l'ARTCI est fixé à Abidjan. Il peut être transféré en tout autre lieu du territoire national, après avis conforme du Conseil de Régulation.

– L'ARTCI est tenue de produire, chaque année, au plus tard le 30 mars, un rapport d'activité. Ce rapport est communiqué au ministre chargé des Télécommunications. Il est publié sur le site Internet de l'ARTCI.

– L'ARTCI est dotée d'un Conseil de Régulation et d'une Direction Générale.

Les Missions

- Définir les principes et autoriser la tarification des services qui sont fournis sous le régime du monopole,
- Délivrer les autorisations d'exploitation des services de Télécommunications,
- Accorder les agréments des équipements terminaux,
- Protéger les consommateurs - Réguler l'internet, la concurrence, l'interconnexion
- Affecter le spectre des fréquences destinées aux acteurs des télécommunications/ TIC.

- Contribuer à l’exercice de toute autre mission d’intérêt public que pourrait lui confier le gouvernement pour le compte de l’Etat dans le secteur des Télécommunications,
- Contribuer à l’exercice des missions de l’Etat en matière de défense et de sécurité Publique, - Réguler le secteur postal, - Protection des données à caractère personnel,
- Gestion des transactions électroniques,
- Gestion des noms de domaines et des adresses Internet de la Côte d'Ivoire, - Gestion

CHAPITRE II : LE CI-CERT

MISSIONS

Le CI-CERT (Côte d'Ivoire – Computer Emergency Response Team) est le CERT national, créé au sein de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire (ARTCI) par le décret n° 2020-128 du 29 janvier 2020 . C'est un centre de veille et de réponse aux incidents de sécurité informatique survenant dans le cyberespace ivoirien.

En sa qualité de centre de coordination des CERT sectoriels nationaux, en abrégé CERT/CC,

le CI-CERT répond aux exigences d'un centre d'opérations de sécurité.

Le CI-CERT collabore avec des organismes afin de collecter et diffuser des informations et coordonner les actions de réponse. Il est également membre du Forum des équipes de réponse aux incidents et de sécurité (FIRST). Le CI-CERT échange des informations avec d'autres CERT et agit comme point de contact pour les incidents de sécurité transfrontaliers.

NOS MISSIONS :

- Assurer la coordination d'une réponse rapide et efficiente en cas d'incident de sécurité informatique ;
- Assurer la veille technologique et le monitoring de sécurité des réseaux et systèmes
  d'information ;
- Assurer la sécurité des systèmes d'information des infrastructures critique d'information ;
- Collecter et traiter les incidents survenant sur les réseaux et systèmes d'information ;
- Assurer la fonction de point focal de la Côte d'Ivoire pour les cas de cybercriminalité ;

- Fournir les moyens techniques nécessaires pour l'échange efficace d'informations en situation de crise ;
- Développer des outils et moyens de sensibilisation des usagers d'Internet, afin de développer la culture nationale de la cybersécurité ;
- Développer des programmes de formation de haut niveau en matière de sécurité des systèmes d'informations ;
- Assurer le développement de la coopération nationale et internationale en matière de cybersécurité.

Le gouvernement ivoirien a donné ce 29 janvier au CI-CERT (Côte d'Ivoire Computer Emergency Response Team) les attributions de point focal national en matière de cybersécurité. Ce qui était naguerre une cellule du régulateur des télécommunications (ARTCI) devient officiellement le gendarme du net en Côte d'Ivoire.

Par le passé, le CI-CERT était à l'ARTCI, la cellule chargée de veiller à la cybersécurité. Son rôle se limitait à recueillir des plaintes, de les acheminer à la police via la DITT (Direction de l'informatique et des traces technologiques) et de faire de la sensibilisation pour éviter de nouvelles victimes de cyberescroquerie. Ses attributions n'étaient pas garanties par une loi ou un décret pris en conseil des ministres.

Depuis ce mercredi « un décret portant création, organisation et fonctionnement du Centre de veille et de réponse aux incidents de sécurité informatique, dénommé « Côte d'Ivoire Computer Emergency Response Team », en abrégé CI-CERT » est venu appuyer ses compétences en matière de lutte contre la cybercriminalité.

Territorialité

Le CI-CERT »a compétence sur l'ensemble de la communauté internet nationale ». Ces attributions s'appliquent toutes les fois où un cybercriminel opère

à partir de la Côte d'Ivoire indépendamment de sa nationalité. Si le forfait en ligne est manigancé en dehors du pays même par un ivoirien elle n'est pas compétente.
Cybersécurité : le CERT ivoirien trône désormais sur la communauté internet nationale

(CIO Mag) – C'est une mesure à la hauteur des défis qu'impose la cybersécurité. Centre de veille et de réponse aux incidents de sécurité informatique, le CI-CERT (Côte d'Ivoire Computer Emergency Response Team) est officiellement le point focal national en matière de cybersécurité et a désormais compétence sur l'ensemble de la communauté internet nationale.

Ainsi en a décidé le gouvernement ivoirien, en consolidant les attributions du CI-CERT à travers un décret adopté mercredi 29 janvier en Conseil des ministres. Par ce moyen, il confère à cette structure toute l'envergure indispensable pour jouer un rôle prépondérant dans la protection du cyber espace national.

Ces dernières années, la Côte d'Ivoire, comme beaucoup de pays africains et dans le monde, a fait l'objet de nombreuses cyber-attaques. Les dommages pécuniaires provoqués par la cybercriminalité ont atteint la somme de 5,5 milliards FCFA en 2018 contre 3 milliards FCFA en 2017.

La montée significative des crimes en ligne avait déjà nécessité des mesures urgentes entre 2012 et 2017. Y compris le renforcement du cadre organisationnel en vue de lutter efficacement contre ce phénomène.

Cyber-pompier

Mais sur les bords de la Lagune Ebrié, la nécessité de créer un CERT a été perçu dès 2009 par les décideurs locaux. Pour améliorer l'image de marque de la Côte d'Ivoire sur les places numériques mondiales. Dix ans après sa création par l'Autorité de régulation des Télécommunications/TIC de Côte d'Ivoire (ARTCI), le CI-CERT mène une série d'activités. Avec un portefeuille de services réactifs et proactifs. Ainsi qu'un service de management de la qualité de la sécurité orienté sur la sensibilisation et la formation.

Il peut s'enorgueillir d'avoir favorisé le recrutement de Responsables de sécurité de systèmes d'information (RSSI) par des opérateurs télécoms, des banques et plusieurs groupes d'entreprises.

En 2018, le CI-CERT a traité plus d'un million d'incidents informatiques. Soit une baisse de 3,7% comparé à l'année 2017. Ces incidents sont constitués à 86,72% d'adresses IP « blacklistées » ; 5,21% sont liés au Botnet, terme utilisé dans le milieu pour désigner un réseau d'ordinateurs infectés par un logiciel malveillant.

Le CI-CERT lutte également contre la cybercriminalité dans le cadre de la Plateforme de lutte contre la cybercriminalité (PLCC), grâce à une convention de partenariat entre la Police nationale, le Parquet d'Abidjan et l'ARTCI.