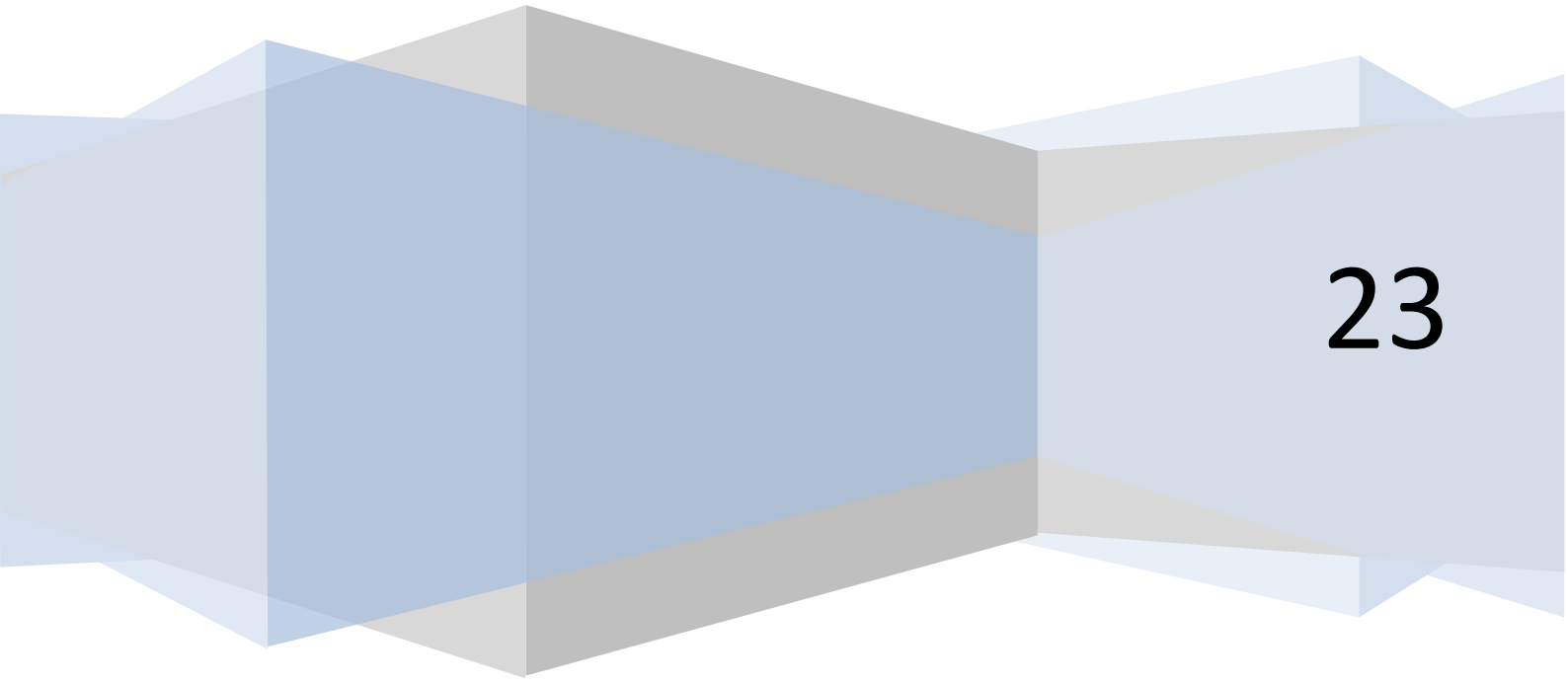
Institut Supérieur du Numérique

Année universitaire 2022-2023

Droit de l'informatique

Droit orienté vers les Nouvelles Technologies de l'Information et de la Communication



23

- **Définition droit de l'informatique** :

Le **droit de l'informatique**, dont le périmètre n'est au demeurant pas strictement défini, recoupe et recouvre donc dans une large mesure **le droit de NTIC**, **le droit des télécommunications**, **le droit de l'internet**, le **droit du commerce électronique** ou encore le « **droit du numérique** ».

En effet, le droit de l'informatique est une discipline spécialisée du droit. C'est l'ensemble des règles de droit applicables aux activités utilisant l'outil informatique.

- **Objectifs :**

Appréhender les enjeux humains et sociaux liés au développement des Nouvelles Technologies de l'Information et de la Communication c'est-à-dire cerner l'impact de la manipulation de droit de l'informatique sur **la société** et sur **l'homme.**

MATIERE PLURIDISCIPLINAIRE

- Droit de la propriété littéraire et artistique,
- Droit d'auteur,
- Droit de la propriété industrielle,
- Brevet d'invention,
- Droit civil et commercial (contrats informatiques),
- Droit pénal (contrefaçon; intrusion frauduleuse dans un système de données),
- Droit international (conflits de loi Cybercriminalité internationale).

QUESTION :

1- Quelle est la particularité du droit de l'informatique ?
2- Comparaison par rapport à d'autres matières de droit ?
3- Le droit de l'informatique est-il figé ?

REPONSE :

1- Le Droit de l'informatique est une matière qui ne figure pas dans un seul code. Elle trouve ses sources dans des textes juridiques divers tels que : **le code de commerce**; le **Code des Obligations et des Contrats** (code civil); **le code pénal**; la **propriété intellectuelle** etc.
2- C'est une matière qui est internationale car la **commission de l'infraction** se fait souvent à travers le territoire de plusieurs Etats.
3- Les nouvelles technologies de l'information et communication sont en constante évolution et le droit doit s'adapter à la technicité de la matière. **Nouvelles formes d'infraction** (intrusion dans les systèmes de données, téléchargement illicite etc.)

Quelques définitions :

- **Droit des NTIC :** Le droit des NTIC, dont le périmètre n'est au demeurant pas strictement défini, recoupe et recouvre donc dans une large mesure le droit de l'informatique, le droit des télécommunications, le droit de l'internet, le droit du commerce électronique ou encore le « droit du numérique ». C'est-à-dire l'ensemble des dispositions normatives et jurisprudentielles relatives aux NTIC. Il tire son originalité de l'approche sur l'information et la technique.

- **Droit de l'Internet** : suggère le même objet d'étude du droit de l'informatique mais auquel on a voulu accentuer le volet des télécommunications et de l'espace virtuel, matérialisé par les sites web.

- **L'Information** : c'est un bien ou une donnée qui se crée et s'échange. Ainsi donc, sans machine l'information n'est rien car pour qu'elle existe elle droit être créée, traitée et transmise.

- **Système Informatique** : tout dispositif isolé ou tout ensemble de dispositifs interconnectés ou apparentés qui assurent ou dont un ou plusieurs éléments assurent, en exécution d'un programme en tout ou partie, un traitement automatisé de données, autrement dit, l'ensemble de matériels (ordinateur, réseaux) et de logiciels permettant d'acquérir, de stocker, de traiter des données pour répondre aux besoins en informations des utilisateurs.

- **Droit d'accès** : conditions nécessaires à l'utilisateur pour accéder à des données protégées. L'on dispose du droit d'accès et de mise à jour de données personnelles nominatives ainsi que du droit de demander leur suppression, l'utilisateur devra alors être identifié. Les droits d'accès sont prédéfinis par administrateur.

- **Accès illicite** : accès intentionnel, sans en avoir le droit, à l'ensemble ou à une partie d'un réseau de communications électroniques, d'un système d'information ou d'un équipement terminal (ordinateur ou mobile par exemple).

- **Droit de la Cybercriminalité :** l'ensemble des infractions s'effectuant à travers le cyberespace par des moyens autres que ceux habituellement mis en œuvre et de manière complémentaire à la criminalité classique.

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

- **Acte criminel:** les actes criminels sont des infractions graves et sont punissables par des peines plus lourdes que les infractions punissables par téléphone ni par courrier.

- **Amende :** peine infligée à la personne condamnée l'obligeant à payer une somme d'argent précise. Habituellement, un délai est accordé à la personne condamnée

pour effectuer le paiement, mais si elle ne paye pas l'amende dans ce délai, elle devra purger sa peine en prison.

- **Citation à comparaître** : formule délivrée par un policier pour obliger un accusé à se présenter devant le tribunal. La citation à comparaître précise la date, l'heure et le lieu de l'audience en cour. Le défaut de s'y conformer peut entraîner la délivrance d'un mandat d'arrestation contre l'accusé.

- **Mandat d'arrestation** : ordre délivré par le tribunal ordonnant l'arrestation d'une personne.

- **Ministère public** : (parquet / magistrat debout) exerce une mission de sauvegarde des intérêts généraux de la société devant le tribunal représenté par des fonctionnaires de police.

- **Témoin :** personne qui témoigne dans un procès. Le témoin est obligé par la loi de comparaître à des dates, heure et lieu précis. Le défaut de comparaître peut entraîner la délivrance d'un mandat d'arrestation contre le témoin.

- **Sommation** : ordonnance obligeant l'accusé à comparaître en cour pour répondre des accusations qui pèsent contre lui. La sommation précise la date, l'heure et lieu de l'audience. Le défaut de comparaître peut entraîner la délivrance d'un mandat d'arrestation.

- **Données informatiques :** toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris tout programme de nature à faire en sorte qu'un système informatique exécute une fonction;

- **Données relatives aux abonnés** : toute information, sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de services et se rapportant aux abonnés de ses services, autres que des données relatives au trafic ou au contenu, et permettant d'établir :

  - le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service;
  - l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de services ;
  - toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de services;

- **Données relatives au trafic** : toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, la taille, l'heure, la date et la durée de la communication ou le type du service sous-jacent;

- **Fournisseur de services** : toute entité publique ou privée qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique ou toute autre entité traitant ou stockant des données informatiques pour ce service de communication ou ses utilisateurs ;

- **Message de données** : toute information créée, envoyée ou reçue par des procédés ou moyens électroniques ou optiques ou des procédés ou moyens analogues, notamment, l'échange de données informatisées, la messagerie électronique;

- **Mineur :** toute personne qui n'a pas atteint l'âge de majorité conformément aux lois et règlements en vigueur en République Islamique de Mauritanie ;

Introduction générale

La réalisation d'un cours relatif au droit de l'informatique, tels que la connectivité de notre pays au réseau international à haut débit, via le câble sous-marin ACE, et le projet de connectivité nationale en cours d'exécution WARCIP Mauritanie, stimulera sans doute, le développement de l'usage de droit de l'informatique dans notre société.

Ce développement contribuera d'une manière considérable, à l'élargissement du champ d'action des opportunités d'échange d'informations de communication et du système.

Une telle situation est susceptible d'engendrer de nouveaux faits et comportements répréhensibles, comme ce fut le cas dans toutes les sociétés avancées en la matière.

Ces nouveaux comportements répréhensibles ont besoin d'être pris en compte par le législateur afin d'être incriminés et sanctionnés.

Dans l'environnement juridique mauritanien, la commission d'infractions portant atteintes aux personnes et aux valeurs morales, par le biais de l'usage de l'infomatique, n'a été mentionnée que dans l'ordonnance n°2005-015 portant protection pénale de l'enfant (articles 47 et 48) et dans la loi n°2010-035 du 21 juillet 2010 abrogeant et remplaçant la loi n°2005- 047 du 26 juillet 2005 relative à la lutte contre le terrorisme.

En dehors de ces dispositions, aucune infraction pénale n'est prévue, d'une manière explicite, en la matière par le code pénal et les autres textes en vigueur.

Face à ces lacunes de l'édifice pénal, il est apparu nécessaire de mettre en place un cadre juridique cohérent de prévention, de dissuasion et de répression de la cybercriminalité dans notre pays.

Et c'est ainsi que la loi N°007-2016, met en place le dispositif juridique de lutte contre la cybercriminalité, et apporte des innovations majeures par l'introduction de nouvelles infractions spécifiques au de l'imformatique, en instituant la protection pénale des systèmes et données informatiques et la répression des infractions se rapportant aux contenus.

Ce nouveau dispositif juridique de lutte contre la cybercriminalité, consacre également une amélioration du cadre processuel, par l'admission de la perquisition et de la saisie informatique, et par l'introduction de nouveaux mécanismes de recherche de la preuve numérique.

Enfin, face à l'internationalisation de la cybercriminalité, une obligation générale de coopération à la charge de notre pays a été consacrée, pour les besoins de la répression des actions cybercriminelles.

En réalité, les thèmes suivants seront notamment être abordés :

I- La protection des personnes (données personnelles automatisées, fichiers, libertés, protection des mineurs) ;

II- La protection des consommateurs (jeux, ventes à distances) ;

III- La sécurité des systèmes et des données (cryptologie, mot de passe, code, signature électronique, licence...) ;

IV- La protection des créations intellectuelles : logiciels, bases de données, produits multimédias) ;

V- Aspects contractuels des NTIC (obligations particulières s'imposant aux informaticiens, les principaux types de contrats, les prestations informatiques, licence, Fournisseurs d'accès à Internet (FAI), maintenance, infogérance...) ;

VI- 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 « Fournisseurs d'accès à Internet », hébergeurs) ;

Chapitre 1 : LA SOCIETE DE L'INFORMATION

Introduction :

Au fil de l'histoire les Nouvelle 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 de droit de l'informatique principal élément utilisé dans une SOCIETE DE L'INFORMATION (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 Système Informatique 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.

SECTION I- Les besoins dans les sociétés informatisées (cas de la Mauritanie).

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

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

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

- Promouvoir l'utilisation de l'informatique afin d'améliorer le rendement dans la société.
  en outre, l'utilisateur doit s'avoir exploité l'information pour son bien être;

- La production et l'utilisation de logiciels doit être encouragé y compris par les autorités publiques ;

- Les infrastructures des NTIC doivent être accessibles en Mauritanie 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 mauritaniens doivent avoir accès aux réseaux d'information à travers les bibliothèques électroniques ;

- L'élaboration des textes, lois et règlements par les autorités compétentes liées à l'usage des NTIC ;

- Inciter les opérateurs de télécommunications et les consommateurs à dénoncer les pratiques et les comportements illicites liés à l'usage des NTIC ;

- La convergence des systèmes économique, politique, culturels en ratifiant les accords internationaux d'échanges en éliminant totalement les droits de douane.

  Les mauritaniens pourront ainsi se doter des capacités nécessaires afin d'accéder à l'ère nouvelle appelée âge de l'information, l'âge de la connaissance.

SECTION II- Informatique et secteurs liés au développement dans la société 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, Territoire, éducation, formation, web 2.0 (désigne l'ensemble des technologies et des usages de la world wibe web car à la différence du web 1.0 où la plupart des 6 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 autocar) 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.

SECTION III- Application des droits dans une société de l'information :

Une protection de l'individu contre la mauvaise utilisation des nouvelles 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 rappeler cette belle expression du philosophe la cardère (19eme siècle) « entre le faible et le fort c'est la loi qui libère ». La préoccupation essentielle du droit est à la fois de prohiber certains comportements et de maintenir certaines valeurs.

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 nouvelles 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.

Section I. Quelques techniques d'atteintes les plus répandues

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 à savoir :

1- L'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 ensuite s'en servir pour contacter des crédits, effectuer des virements ou prendre des abonnements téléphoniques.

2- 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 ;

3- Le harponnage ou spear- phishing :

C'est une 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;

4- 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;

5- 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.

SECTION II. Responsabilité civile et pénale

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 soient 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 leurs personnes d'une alternative entre la voix pénale et la civile pour obtenir une condamnation de la coupable et éventuelle réparation.

A- La responsabilité pénale.

Le droit pénal mauritanien, 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 :

1- **Une contravention :** (infraction sanctionnée par une amende) Tribunal de police à compétence en ces cas.

2- **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.

3- **Un crime :** (homicide, action blâmable) la cour d'assise composé d'un jury populaire
La loi mauritanienne n° 2016/07 relative à la cybercriminalité prévoit que les sanctions varient selon que l'intrusion a eu ou non une incidence sur le système mis en cause.

Il existe trois types d'intrusion dans un système automatisé de données :

On peut citer pour illustration quelques sanction en la matière du droit français :

- **Les intrusions simples :**

L'article 323-1 du code pénal français dans la section « des délits contre les systèmes de traitement automatique de données » prévoit que « le fait d'accéder ou de se maintenir, frauduleusement dans tout ou partie d'un système de traitement automatique de données est puni de 2 ans d'emprisonnement et de 30.000 euros d'amende ».

- Les intrusions avec dommages :

L'alinéa 2 de l'article 323-1 prévoit un renforcement de sanction lorsque l'intrusion et le maintien frauduleux on certains conséquences : « Lorsqu'il en résulte soit la suppression soit la modification de données contenues dans les systèmes, soit une altération du fonctionnement du système, la peine est de 3 ans d'emprisonnement et de 45.000 euros d'amende ».

- Les entraves volontaires au système et aux données s'y trouvant :

L'article 323-2 définit l'entrave volontaire au système comme « le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de 5 ans d'emprisonnement et de 75.000 euros d'amende ».

Cette intrusion vice notamment l'introduction des programmes susceptibles d'entrainer une perturbation au système tel que les virus. illustration d'un cas d'usurpation d'identité Une personne qui se dit victime d'usurpation d'identité dispose d'un délai de 3 ans pour ester en justice, dépasser ce délai sa requête sera caduque.

B- La Responsabilité civile :

Le droit civil français à un caractère strictement compensatoire puisqu'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 a 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 :**

1-Un préjudice subi par la victime.
2-Une faute de l'auteur du délit.
3-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.

SECTION III. Les techniques de sécurité dans un système 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 périodiques 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 :

1- La notion de session c'est-à-dire l'authentification de l'utilisateur qui est à la base du mécanisme de sécurité de Windows.

2- Interdiction du partage des comptes (création de plusieurs comptes, désactiver les comptes inutilisés).

3- Activer les fonctions essentielles de sécurité c'est-à-dire activée le pare-feu/firewall (barre de tache-alerte de sécurité windows-protection pare-feu- activer) ou bien panneau de configuration et activer).

La notion de sécurité dans un navigateur à l'exemple d'internet explorer (outil-option internet- paramétrer les options de sécurité (sécurité + avancé...).

C- La protection logique.

1- L'installation des programmes antivirus :

2- L'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.

3- 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.

4- 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.

5- 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 réparer et à supprimer les spywares qui pullulent sous Windows Exemple : AVG (anti-spyware).

6- 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 d'accès.

CHAPITRE III : 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 français et l'article 23 du Code des obligations et des contrats en Mauritanie :

- **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.

Section 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'info gérant 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.

Section 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 soumis 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 cocontractants ;**
- **Le prix :** il peut être indiqué sous forme forfaitaire ou à l'unité les conditions de payement et les pénalités doivent être prévues ;