Chapitre III : CRIMINALITE INFORMATIQUE

La criminalité informatique ne recouvre pas une catégorie d'infractions clairement définie, mais un ensemble flou d'activités illicites liées à 1'informatique. Elle est un vaste domaine, dont les frontières ne sont pas toujours faciles à définir. Chaque pays à une législation différente a ce sujet.

La montée de la délinquance informatique engendrée par le développement rapide des sciences de l'information et des nouvelles technologies de communication inquiète de plus en plus les pays, les organisations, les services de police et les particuliers concernés. Ces dernières années cette criminalité qui menace la sécurité de la société de 1'information a été prise très au sérieux par les autorités de justice de tous les pays.

La plupart des spécialistes ont tendance à proposer une classification qui distingue les affaires ou 1'ordinateur ou le réseau informatique sont la cible de celles dans laquelle 1'ordinateur ou le réseau informatique sont les instruments. Le système de codification des infractions informatiques du Secrétariat général d'Interpol recense près de trente types d'infractions.

Parmi toutes ces types d'infractions informatiques, les cas des intrusions informatiques, des piratages téléphoniques, des virus informatiques et de la pédophile sur Internet sont la criminalité informatique la pus fréquente.

Pour mieux se protéger des pirates, mieux vaut bien les connaitre. Donc il est indispensable de savoir les motivations, les techniques, les comportements et les moyens des criminels informatiques pour établir les mesures techniques et juridiques de protection et de prévention susceptibles de réduire les risques.

La cybercriminalité est l'une des formes de criminalité qui connaît actuellement une forte croissance, les criminels exploitant la rapidité et la fonctionnalité des technologies modernes ainsi que l'anonymat qu'elles permettent pour commettre leur activité illicite en tous points du globe : piratage des données et des systèmes informatiques, vol d'identité et escroqueries aux enchères sur le net. En effet, le vol de données personnelles, l'altération de logiciels, la prise de contrôle de sites officiels, les détournements de fonds et les escroqueries commerciales…etc.

1-Présentation de La Criminalité Informatique

La criminalité informatique regroupe les infractions pénales qui sont commises à l'encontre de données informatiques ou d'un système informatique généralement connecté à un réseau.

L'une de ces infractions est le **faux informatique**. À l'instar du faux en écriture, le faux informatique implique l'altération de la vérité. Cependant, la vérité qui est altérée n'est ici pas contenue dans un acte écrit, mais dans des données informatiques. **L'usage d'un faux informatique** est également érigé en infraction pénale.

La **fraude informatique** correspond en quelque sorte à une variante de l'escroquerie. On parle de fraude informatique lorsque l'avantage illicite a été poursuivi par la tromperie non d'une personne, mais d'une machine. Ainsi, l'utilisation de moyens de communication modernes pour tromper une personne n'en demeure pas moins une escroquerie et non une fraude informatique.

Le **hacking** désigne le fait d'accéder, sans y être autorisé, à un système informatique. Le Code pénal fait une distinction entre le hacking perpétré par une personne qui ne dispose pas du tout d'une autorisation d'accès au système en question et celui perpétré par une personne qui y a un accès limité mais qui transgresse cette limitation.

Enfin, le **sabotage informatique** vise la modification voire la destruction de données ou d'un système informatique. A nouveau, l'objet du sabotage doit consister en des données ou un système informatique de sorte que si le sabotage porte uniquement sur un support informatique, comme un ordinateur, il n'y a pas sabotage informatique.

1.1.Le faux informatique et l'usage de faux informatique

À l'instar du faux en écriture, le faux informatique implique l'altération de la vérité. Dans le cadre du faux en informatique toutefois, cette vérité n'est pas contenue dans un acte écrit, mais dans des **données informatiques**. En outre, il faut encore que ces données aient une portée juridique, c'est-à-dire qu'elles puissent

servir de fondement à l'exercice d'un droit ou d'une action, à constater ou à prouver un droit.

Du point de vue matériel, le faux informatique peut prendre la forme de **l'introduction, la modification ou la suppression de données dans un système informatique ou la modification, par tout moyen technologique, de l'utilisation possible des données dans un système informatique**. Selon les travaux parlementaires, les termes 'introduction', 'modification' et 'suppression' doivent recevoir une interprétation la plus large possible.

L'infraction de faux informatique est également composée d'un élément moral particulier, il faut nécessairement que son auteur ait agi avec la conscience d'altérer la vérité et une intention particulière. Cette intention peut soit être **frauduleuse**, c'est-à-dire l'intention de se procurer ou procurer à autrui un avantage illégal, soit à **dessein de nuire** à autrui.

Les **peines prévues** par le législateur sont l'emprisonnement de six mois à cinq ans et l'amende de vingt-six à cent mille euros ou l'une de ces peines seulement. En cas de récidive dans les cinq ans d'une précédente condamnation telle que définie par la loi, les peines mentionnées sont doublées [5]. Enfin, la tentative de faux informatique est punie d'un emprisonnement de six mois à trois ans et d'une amende de vingt-six à cinquante mille euros ou d'une de ces peines seulement.

Le législateur incrimine également **l'usage de faux informatique**. Ainsi, celui qui fait usage des données obtenues illégalement, tout

en sachant que celles-ci sont fausses, est puni comme s'il était l'auteur du faux.

Un exemple de faux et usage de faux informatique est le **skimming**. Cette pratique consiste à copier la bande magnétique d'une carte de banque. Lorsque les clients retirent de l'argent sur un distributeur, des appareils de lecture installés par les faussaires copient la bande magnétique dès que la carte est introduite dans le distributeur. Les données récoltées illégalement sont ensuite copiées sur une carte vierge. Pour obtenir le code PIN nécessaire à l'utilisation de la carte, des caméras cachées ou un clavier falsifié sont souvent utilisés. La carte bancaire qui est ainsi copié répond à la qualification de faux, c'est-à-dire une imitation de la vérité, de la carte authentique.

1.2. La fraude informatique

Avec le développement des nouvelles technologies, il était temps d'actualiser l'arsenal pénal que constitue le Code pénal. L'une des avancées en la matière est l'instauration de l'infraction de fraude informatique qui vise en quelque sorte le cas d'une escroquerie lorsque l'avantage illicite a été poursuivi par la **tromperie non d'une personne, mais d'une machine**.

Concrètement, la fraude informatique sanctionne le fait **d'introduire, de modifier ou d'effacer des données dans un système informatique ou de modifier l'utilisation normale de ces données**. Encore, la définition des termes utilisés par le législateur est extrêmement large puisque tout traitement ou manipulation de données dans un

système informatique répond à la qualification de fraude informatique. Cela implique qu'il n'est pas rare que les infractions de fraude informatique et de faux informatiques soient concomitantes.

Toujours selon les termes de la loi, l'auteur doit **chercher à se procurer un avantage économique illégal**. Le simple fait de rechercher un tel avantage est en soi incriminé quand bien même cet avantage n'aurait finalement pas été obtenu. Cet élargissement du champ d'application de l'infraction ne paraît toutefois pas indispensable dans la mesure où le législateur incrimine également la tentative de fraude informatique. L'auteur d'une telle tentative peut être sanctionné d'un emprisonnement de six mois à trois ans et d'une amende de vingt-six à cinquante mille euros ou à l'une de ces peines seulement.

Sur le plan moral de l'infraction, le fraudeur doit agir avec une **intention frauduleuse**, à savoir l'intention de se procurer ou procurer à autrui un avantage illégal. À titre d'illustration, pareille intention ne peut être constatée dans le chef de celui qui retire de l'argent d'un compte bancaire et qui dépasse involontairement le crédit de ce compte.

L'auteur d'une fraude informatique encourt une peine d'**emprisonnement** de six mois à cinq ans et/ou une **amende** de vingt-six à cent mille euros. En cas de récidive dans les cinq ans d'une précédente condamnation telle que définie par la loi, les

peines mentionnées tant pour la fraude que pour la tentative de fraude sont doublées.

1.3. Le hacking

L'accès non autorisé à un système informatique, ou *hacking*, est érigé en infraction au sein du Code pénal. Cette pratique désigne le fait de s'introduire dans le système informatique de quelqu'un à son insu, sans disposer de l'habilitation requise.

En fait, il faut faire une distinction entre le hacking externe et le hacking interne.

Le **hacking externe** est le fait d'une personne étrangère au système informatique piraté. Ce comportement est érigé en infraction lorsque l'auteur, sachant qu'il n'y est pas autorisé, accède ou se maintient dans un système informatique. Ce qui est intéressant c'est que le simple accès ou le maintien suffit pour que l'infraction soit consommée. Il n'est donc pas requis que l'auteur cause un quelconque dommage. L'existence d'un dommage constitue par contre une circonstance aggravante tant pour le hacking externe que pour le hacking interne. L'auteur d'un hacking externe encourt une peine d'emprisonnement de trois mois à un an et/ou une amende de vingt-six à vingt-cinq mille euros. En cas d'**intention frauduleuse** constatée dans son chef, la peine d'emprisonnement est de six mois à deux ans.

Le **hacking est interne** lorsqu'il est commis par une personne ayant accès au système informatique mais qui a outrepassé les limites de

son autorisation. À nouveau l'existence d'un éventuel dommage causé n'intervient qu'à titre de circonstance aggravante. Par contre, le législateur exige que le hacker ait agi avec une **intention frauduleuse** ou dans le **but de nuire** pour que son comportement puisse être incriminé. Dans pareil cas, l'auteur peut être condamné à une peine d'emprisonnement de six mois à deux ans et/ou à une amende de vingt-six à vingt-cinq mille euros.

À côté du **dommage causé**, deux autres circonstances aggravantes communes aux deux types de hacking ont été prévues. Il s'agit d'une part de la **prise ou du vol de données**. La simple prise de connaissance de ces données suffit mais généralement, l'auteur en fait une copie sur un support numérique. Cette pratique se rencontre souvent en matière d'espionnage industriel. D'autre part, **l'utilisation du système piraté** constitue également une circonstance aggravante. Dans ces trois cas aggravés, les peines sont l'emprisonnement de un à trois ans et/ou l'amende de vingt-six à cinquante mille euros.

Le législateur a également érigé en infraction la **tentative de hacking**. Cette tentative est sanctionnée des mêmes peines que le hacking-même. En outre, la **récidive**, la **préparation** d'un hacking, sa **provocation** ainsi que le **recel** des données informatiques obtenues à la suite d'un hacking sont pénalement sanctionnés.

1.4.Le sabotage informatique

A la différence d'autres infractions informatiques, le sabotage informatique n'a pas nécessairement pour but un enrichissement. Il peut y avoir sabotage informatique lorsqu'une personne insère un virus ou un cheval de Troie dans un système informatique même sans en tirer d'avantage financier.

Commet un sabotage celui qui, **sans y être autorisé, introduit, modifie ou efface des données dans un système informatique ou qui modifie par tout moyen technologique l'utilisation normale de données dans un système informatique**. À nouveau, ce qui est important, ce sont les notions de données et de système informatiques. La destruction d'un ordinateur n'est donc pas un sabotage, mais la destruction d'un bien appartenant à autrui.

2-Le Droit Pénal National Face a La Nouvelle Criminalité

Le code pénal algérien a partir de la révision de 2004, à pris en considération la criminalité informatique, dans la section 07 sous-titre « **Atteintes à la propriété littéraire et artistique** », le titre de la section 07 bis et « **des atteintes aux systèmes de traitement automatisé de donnée** ».

A partir de L'article 394 bis le législateur puni d'une peine d'emprisonnement de (03) mois à un (01) an et d'une amende de 50.000 DA à 100.000 DA, quiconque accède au se maintient, frauduleusement, dans tout ou partie d'un système de traitement

automatisé de données, ou tente de le faire. (**Le hacking ou bien L'accès non autorisé à un système informatique**)

Lorsqu'il on est résulté une altération du fonctionnement de ce système, la peine est de six (06) mois à deux (02) ans d'emprisonnement et d'une amende de 50.000 DA 0 150.000 DA. (**Le sabotage**)

L'article 394 ter. Est puni d'un emprisonnement de (06) mois à trois (03) ans et d'une amende de 500.000 DA à 2.000.000 de DA, quiconque introduit frauduleusement des données dans un système de traitement automatisé ou supprime ou modifie frauduleusement les données qu'il contient. (**Le faux informatique et l'usage de faux informatique**)

L'article 394 quater. Est puni d'un emprisonnement de (02) mois à trois (03) ans et d'une amende de 1.000.000 de DA à 5.000.000 de DA, quiconque volontairement et frauduleusement ; rassemble, met à disposition, diffuse, commercialise des données qui en stockées, divulgue….etc (**La fraude informatique**)

Les peines sont portées au double lorsque l'infraction porte atteinte à la défense nationale aux organismes ou établissements de droit public, sans préjudice de l'application des peines plus sévère (article 394 quinquiès).

L'monde sera équivalent à cinq (05) fois le maximum de l'amende prévue pour la personne physique, c'est l'infraction commis par une personne morale (article 394 sixiès).

Enfin la tentative des délits prévue à la présente partie est punie des mêmes peines prévues pour le délit lui-même.

3-La Protection Pénal du L'informatique par L'ordonnance 03-05

L'ordonnance 03-05 considère qu'il est coupable du délit de contrefaçon qui conque :

— divulgue illicitement une œuvre ou porte atteinte à l'intégrité d'une œuvre ou d'une prestation d'artiste interprète ou exécutant ;

— reproduit une œuvre ou une prestation par quelque procédé que ce soit sous forme d'exemplaires contrefaits ;

— importe ou exporte des exemplaires contrefaits d'une œuvre ou prestation ;

— vend des exemplaires contrefaits d'une œuvre ou prestation ;

— loue ou met en circulation des exemplaires contrefaits d'une œuvre ou prestation. (Article 150)

Est aussi coupable du délit de contrefaçon, quiconque, en violation des droits protégés en vertu de la présente ordonnance, communique l'œuvre ou la prestation, par représentation ou exécution publique, radiodiffusion sonore ou audiovisuelle, câblodistribution ou tout autre moyen transmetteur de signes porteurs de sons ou d'images ou sons ou par tout système de traitement informatique.(Article 151)

La contrefaçon est une infraction pénale, Il s'agit d'un délit passible d'une peine d'emprisonnement de six (6) mois à trois (3) ans et

d'une amende de cinq cent mille (500 000 DA) à un million (1.000. 000 DA) de dinars que la publication ait lieu en Algérie ou à l'étranger. (Article 152)

*Remarque :Le champ de la contrefaçon en informatique est plus vaste car celle-ci englobe tous ce qui concerne le matériels et composants électronique(Ce point couvre tout ce qui concerne la fabrication des ordinateurs et de leurs périphériques : cartes mères, cartes sons, disques, etc.) Il s'agit ici de matériels parfaitement bien protégeables par des brevets. En rajoute les logiciels qui sont protégés par le droit d'auteur.