# SEQUENCE 1 : INTRODUCTION GENERAL AU DROIT DES TIC

## CLASSIFICATION DES INFRACTIONS SUR INTERNET

Quel que soit les méthodes utilisées dans le cadre de cette modernisation des infractions les TIC constituent le moteur principal. En effet les délits de la cybercriminalité se divisent en deux catégories d'infractions :

- Les infractions où les TIC sont l'objet du délit
- Les infractions où les TIC sont le moyen du délit

### A- LES TIC : OBJET DE COMMISSION DES CYBERINFRACTIONS

Toutes les infractions classées dans cette catégorie portent atteinte à au moins l'un des trois principes juridiques que sont la confidentialité, l'intégrité et la disponibilité. Les systèmes et les données informatiques sont apparus il y a des années au Sénégal. Contrairement aux délits traditionnels (vols, meurtres, etc.), qui entrent dans le champ d'application du droit pénal depuis des lustres, les infractions informatiques sont donc relativement récentes. Pour pouvoir engager des poursuites contre les auteurs de ces actes, il est nécessaire que le droit pénal en vigueur contienne des dispositions visant à protéger les objets tangibles et les documents matériels contre la manipulation, mais aussi que ces dispositions englobent les nouveaux principes juridiques susmentionnés. Ainsi pour une meilleure perception de cette section, il conviendra de parler en premier lieu des infractions liées aux données informatisées (1) et en second lieu des infractions liées aux systèmes informatiques (2).

#### 1 : LES ATTEINTES LIEES AUX NOUVELLES TECHNOLOGIES

De nos jours, avec l'avènement du phénomène de la cybercriminalité, elles sont souvent utilisées comme objet de commission d'infractions par le biais des TIC. En effet, il existe de nouvelles incriminations spécifiques à ces dernières qui portent atteintes aux données informatiques. Ces diverses infractions s'articulent autour de la confidentialité et l'intégrité des données. Tout d'abord, parmi les atteintes liées à la confidentialité des données, nous avons :

- L'interception ou la tentative d'interception des données informatisées : intercepter signifie arrêter quelque chose au passage, en interrompre le cours direct. peut être considérée comme un accès avec modification des informations transmises sur les voies de

communication avec l'intention de détruire les messages, de les modifier, d'insérer des nouveaux messages, de provoquer un décalage dans le temps ou la rupture dans la diffusion des messages. Mais pour qu'elle soit vue comme une infraction, l'interception doit être effectuée sans autorisation. En somme, c'est le fait d'intercepter frauduleusement des données informatiques par des moyens techniques lors de leur transmission non publique à destination, en provenance ou à l'intérieur d'un système informatique.

Ces infractions sont punies par la loi sénégalaise sur la cybercriminalité de 2008 ainsi que par la constitution.

- Ensuite il y a des atteintes liées à l'intégrité des données qui sont définies comme « l'altération ou l'entrave au fonctionnement du système d'information. » L'altération au fonctionnement est toute action consistant à fausser le fonctionnement dudit système pour lui faire produire un résultat autre que celui pour lequel il est normalement conçu et utilisé. L'entrave au fonctionnement elle, toute action ayant pour effet, objet ou finalité de paralyser un système d'information l'introduction, la transmission, l'endommagement, l'effacement, la modification, l'altération ou la suppression des données.

**2 : LES ATTEINTES LIEES AUX SYSTEMES INFORMATIQUES**

Est qualifiée de système informatique « tout dispositif isolé ou non, tout ensemble de dispositifs interconnectés assurant en tout ou partie, un traitement automatisé de données en exécution d'un programme. ». Cette définition a aussi été utilisée dans les conventions de Budapest en 2001 et de Malabo en 2014 ainsi que dans la directive de la CEDEAO de 2011. Il peut s'agir d'un ordinateur, d'un réseau de télécommunication ou d'une carte à puce etc. Pour qu'il puisse bénéficier d'une protection pénale, le système informatique doit en pratique bénéficier d'un dispositif de sécurité afin que le juge puisse établir la preuve de l'élément moral des atteintes aux systèmes (mot de passe, dispositif de cryptologie etc…) mais en théorie ce dispositif n'est pas indispensable. Les infractions des systèmes s'articulent aussi autour des atteintes à la confidentialité, à l'intégrité mais aussi à la disponibilité des systèmes. Tout d'abord les atteintes à la confidentialité des SI sont traduites par deux infractions :

- L'accès frauduleux à un système informatique : si l'on traduit l'article 431-8 de la loi sur la cybercriminalité ou l'article 4 de la Directive de la CEDEAO, c'est le fait d'accéder ou de tenter d'accéder frauduleusement à tout ou partie d'un SI. Une définition plus précise a été donnée par le Tribunal de Dakar lors d'un jugement du 18 Septembre 2009 : « un accès

frauduleux à un système consiste à une intrusion, une pénétration par une personne dans le système sans y être autorisé, à l'aide de manipulation ou de manœuvre quelconque, c'est-à-dire à l'établissement d'une communication avec le système. ». Il est aussi appelé « hacking » ou piratage informatique. Il peut se faire en forçant ou en contournant le dispositif de sécurité. Le juge sénégalais s'est prononcé plusieurs fois sur ce genre d'infraction. Par exemple, le Tribunal Hors Classe de Dakar dans sa décision n° 4241/ 09 du 18 septembre 2009 a statué sur une affaire dans laquelle le prévenu a été condamné pour avoir accédé frauduleusement à tout ou partie d'un système informatique. En l'espèce, il est reproché au prévenu d'avoir accédé à l'ordinateur d'un collègue et d'envoyer dans sa propre boîte électronique une copie de données de nature commerciale. Le 21 Janvier 2010, le TRHCD s'est prononcé aussi sur une infraction dans laquelle le prévenu a accédé frauduleusement, grâce à des cartes bancaires dupliquées, aux terminaux de paiement électronique d'une grande banque de la place. Ces illustrations montrent que l'accès frauduleux devient de plus en plus fréquent dans notre société.

- Le maintien frauduleux dans un système informatique : a été prévu et réprimé par la législation sénégalaise. Si l'on se réfère à l'article 5 de la Directive de la CEDEAO, il est défini comme « le fait pour toute personne de se maintenir ou de tenter de se maintenir frauduleusement dans tout ou partie d'un système informatique ». La loi n°2014-006 de l'AFPDP sur la lutte contre la cybercriminalité en donne une définition plus précise : « Est qualifié de maintien frauduleux, le fait par toute personne qui, intentionnellement, sans excuse légitime ou justification supérieure d'une excuse légitime ou justification, de rester connecté dans un système informatique ou dans une partie d'un système informatique ou de continuer d'utiliser un système d'information. » . Il en résulte que le maintien doit se faire de manière consciente. Il doit aussi revêtir un caractère intentionnel. Selon le juge Papa Assane Touré « cette infraction réprime le fait pour un individu non habilité, d'avoir accédé par hasard ou par erreur à un système ou bénéficiant d'une autorisation de connexion limitée dans le temps ». Par ailleurs notons qu'un problème de cumul entre l'accès et le maintien frauduleux a été relevé. En effet certains auteurs pensent qu'on ne peut accéder à un système pour en ressortir immédiatement. Donc le caractère de maintien dans le système y est forcément. Cependant d'autres comme le Professeur Raymond Gassinestiment qu'« il ne pourrait avoir de cumul réel d'infractions que lorsqu'un individu qui a accédé frauduleusement à un système se voit sommé d'en sortir par un moyen technique quelconque et s'y maintient cependant malgré cette sommation. »

Ensuite nous avons les atteintes à l'intégrité des données. La notion d'intégrité signifie selon l'article 3 de la loi n° 2008-41 du 20 Août 2008 sur la cryptologie « la propriété qui assure que des données n'ont pas été modifiées ou détruites de façon non autorisée lors de leur traitement, conservation et transmission ». Il existe deux infractions spécifiques aux atteintes à l'intégrité du système :

- L'entrave au fonctionnement du système : Entraver est synonyme d'arrêter, d'empêcher, d'enrayer. L'effectuer au fonctionnement du système est considéré comme les comportements réalisés au moyen d'actions positives, ayant pour résultat d'empêcher l'aboutissement du traitement informatique. Les infections informatiques (virus informatiques, vers informatiques, bombes logiques, chevaux de Troie) en sont de parfaites illustrations. Ceux sont des programmes destinés à perturber le fonctionnement normal du SI. Le Mail-Bombing par exemple consiste à un envoi massif de courriers électroniques peut aussi constituer une entrave s'il a pour effet de perturber le fonctionnement du SI. Dans son jugement du 8 juin 2006[1], le TGI de Nanterre a été confronté à cette pratique. En effet, suite à un différend commercial, une société avait subi plusieurs fois des attaques de type mail-bombing via l'interface du contrat de son site. Après enquête, il a été révélé qu'une personne avait envoyé près de douze mille copies d'un même message et le prévenu a été condamné à deux mois d'emprisonnement avec sursis sur le fondement d'un délit d'entrave au fonctionnement du STAD. La pratique du « spamming » aussi constitue un délit d'entrave. Elle renvoie à « l'envoi massif et parfois répété de courriers électroniques non sollicités, à des personnes avec lesquelles l'expéditeur n'a jamais eu de contact et dont il a capté l'adresse électronique de façon irrégulière ».[2]
- L'action de fausser le fonctionnement du système : c'est l'action sur le système qui, sans empêcher son fonctionnement, lui fait produire un résultat différent de ce qui est escompté. [3]Comme exemple, on peut citer le cheval de Troie. Cette technique consiste à insérer un programme apparemment inoffensif dans un système, qui sera ensuite exécuté comme partie intégrante du programme. Elle peut entrainer la modification imperceptible soit du système d'exploitation soit du programme. L'entrave fait l'objet de confusion avec l'action de fausser le fonctionnement du système du fait qu'elles soient matérialisées parfois par les

[1] TGI Nanterre, 8 Juin 2006 disponible sur www. legalis.net
[2] « Cybercriminalité, défi mondial », 2e édition, Paris, Economica, 2009, P 80 de M.QUEMENER et J. Ferry
[3] « La cybercriminalité dans les législations communautaires intégrées en Afrique » p 9

mêmes exemples mais il reviendra au juge pénal sénégalais de cerner la frontière entre ces deux notions.

Enfin il y a les atteintes liées à la disponibilité du SI. Le terme disponible renvoie à une chose « dont on peut disposer, qu'on peut utiliser librement » selon le dictionnaire français LAROUSSE. La disponibilité du SI peut être considéré comme « le critère de sécurité permettant que les ressources de réseaux de communications électroniques, des systèmes d'information ou des équipements terminaux soient accessibles et utilisables selon les besoins »

- l'introduction frauduleuse de données dans un système informatique : c'est une opération technique consistant à incorporer des caractères magnétiques nouveaux dans un système se traduisant par un changement d'état du SI. C'est-à-dire lorsque des caractères magnétiques nouveaux sont incorporés dans un système, sans que l'on y soit autorisé. Ainsi, à la différence du simple cas d'accès frauduleux à un système informatique, il est noté une introduction ou une tentative d'introduction de données dans le système. Le TGI de Paris s'est déjà prononcé sur ce type d'infraction dans son jugement du 5 Octobre 2010 à propos de l'affaire Kiervel. Il a considéré que le délit d'introduction frauduleuse de données dans un STAD a été commis par le Sieur Kiervel qui a « sciemment saisi des opérations sans réalité économique, qu'il a par la suite pour partie annulée dans le seul but de masquer ses engagement shors mandat et hors limite. » Toutefois, la proximité avec le délit d'accès frauduleux est telle qu'un chevauchement est possible. Ce chevauchement résulterait d'une erreur rédactionnelle que le législateur sénégalais souhaiterait dans la réforme du code pénal et du code de procédure pénale rectifier par souci de cohérence. Cette réforme envisagerait la suppression de la référence à l'accès frauduleux à un système informatique dans les atteintes à la disponibilité des systèmes.