# Droit Electronique : Introduction à la cybercrminalité au Maroc

publié le **29/08/2016**, vu **8419 fois**, Auteur : Fouad Benseghir

**Article traitant d'une introduction technico-juridique de la cybercriminalité au Maroc**

Il va sans que la cybercriminalité occupe une place grandissante dans un monde désormais exposé au développement des technologies de l'information et des télécommunications surtout internet.

Contraction d "inter-Network", internet est couramment défini comme un « ensemble de réseaux informatiques privés et publics connectés entre eux grâce à un protocole de communication commun ».

Si aujourd'hui internet est devenu un vecteur essentiel d'information, de communication et de commerce, il est aussi un territoire propice au développement d'une nouvelle forme de délinquance : la cybercriminalité.

A l'heure actuelle, une grande partie de la population marocaine est connecté à Internet et utilise au quotidien  les services qu'il propose.

En effet, selon le dernier rapport de l'ANRT, le nombre d'abonnés au Maroc dépasse les 16 millions fin 2015.

Le nombre important des utilisateurs d'internet est lié entre autres au phénomène des médias sociaux : Les études récentes indiquent à ce sujet que 73% des internautes marocains utilisent des réseaux sociaux ( Facebook, Twitter, Instagram, MySpace….).

L'accroissement de l'utilisation de l'internet mobile connait aussi un progrès remarquable depuis quelque année. En effet, le nombre de Smartphones en circulation au Maroc dépasse les 16 millions d'unités toujours selon la même étude.

Par ailleurs, la proportion de la population qui dispose d'un téléphone intelligent et l'utilise pour consulter internet est de 65% fin 2015.

Ces utilisateurs ( internautes et mobinautes) représentent désormais une population à part entière, avec autant de victimes potentielles ou de possibles délinquants.

D'un autre côté, les systèmes d'information font désormais partie intégrante du fonctionnement des administrations publiques et de l'activité des entreprises privées.

Pour les besoins de cet Etude, on appelle Système d'information, un ensemble de machines connectées entre elles de façon permanente ou temporaire permettant a une communauté de personnes physiques ou morales d'échanger des données ( textes, images, sons,…).

Selon cette définition, des systèmes aussi variés qu'un téléphone portable, un CD ou DVD, un disque dur, une carte à puce, une clé USB, le réseau d'un opérateur de téléphonie, le site internet d'un ministère, l'ordinateur individuel d'un particulier, le réseau de commandement des forces armées royales…. constituent des systèmes d'information.

Lesdits systèmes d'information privés comme publics sont le plus souvent les cibles d'attaques malveillantes d'origine interne ou même guidées depuis l'extérieur du pays.

En effet, de plus en plus de malfaiteurs exploitent l'immatérialité, l'internationalité et surtout l'anonymat que les technologies de l'information et des télécommunications permettent pour commettre les cyberinfractions les plus diverses.

Ces dernières font référence aux nouvelles formes de délits et crimes qui se produisent dans le cyberespace. Celui-ci pouvant être défini comme un espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numériques.

En référence à cette définition, un cybercrime est définit par les Nations Unies comme « toute infraction susceptible d'être commise à l'aide d'un système ou d'un réseau informatique, dans un système ou un réseau informatique ou contre un système ou un réseau informatique. Il englobe, en principe, toute infraction susceptible d'être commise dans un environnement électronique ».

Ce type de criminalité est l'œuvre d'auteurs ( hackers, crackers, phreakers, hacktivistes….) qui, quoi qu'ils utilisent les mêmes techniques, ils se distinguent du fait qu'ils n'ont pas les mêmes motivations. Toutefois, la loi ne fait pas de distinction entre ces différents types de cybercriminels puisque tous peuvent être poursuivi au regard du code pénal.

Précisons sur ce chef, qu'il est difficile pour ne pas dire impossible d'élaborer une typologie des cybercrimes car quelle que soit l'approche adoptée, il existera toujours des chevauchements.

Toutefois, une classification par domaine touché par ces actes ( infractions touchant aux systèmes d'information, infractions touchant aux données personnelles, infractions touchant à la propriété intellectuelle, infractions touchant aux réseaux de télécommunications, infractions touchant aux intérêts de l'Etat…) peut être à notre sens une base de travail logique pour étudier le phénomène de la cybercriminalité.

La cybercriminalité n'est pas tout à fait une délinquance comme une autre, compte tenu de son aspect technique et de son caractère évolutif qui fait qu'elle gagne en sophistication d'année en année sous l'effet du développement technologique.

On peut citer à cet égard, les nouveaux outils de communication fournit dans le cadre de ce qu'on appelle le WEB 2.0 qui désigne l'Internet liant des personnes ( Blogs, forums, réseaux sociaux…) qui succède à la première version du Web 1.0 celle liant les pages web entre elles à partir des hyperliens, qui sont très exploités par les cybercriminels.

Ces derniers, profitent en effet du potentiel considérable qu'offrent ces outils pour commettre des infractions touchant à presque tous les domaines précités.

Par ailleurs, de nouvelles technologies relevant du monde de l'informatique, des télécommunications et de l'Internet ne cessent d'apparaitre et de créer de nouvelles possibilités mais également de nouveaux risques.

Parmi ces technologies émergentes, nous soulignons notamment l'internet mobile, l'Internet des objets et l'informatique dans le nuage ( Cloud computing ) qui font de plus en plus partie du quotidien des utilisateurs.

Concernant **d'abord** l'Internet mobile, les utilisateurs migrent une part de plus en plus importante de leur vie quotidienne sur leurs appareils mobile. Il est donc normale de prévoir que les cybercriminels dirigeront leurs attaquent vers ce créneau en plein expansion.

Pour ce qui est **ensuite** de l'Internet des objets, ce terme permet de désigner la situation ou une multitude d'objets disposent de connexion sans fil à  Internet capables de dialoguer et d'interagir.

Lesdits objets connectés pourraient être de toutes sortes comme les voitures, les téléphones portables, les appareils électroménagers, les télévisions, les imprimantes…etc.

L'avènement de l'Internet des objets s'accompagnera probablement d'une multitude d'infractions parfois nouvelles ( contrôle à distance des véhicules, utilisation à distance des Smartphones…) mais également anciennes rendues plus efficaces en raison du nombre considérable d'objets connectés.

S'agissant de l'informatique dans le nuage **enfin**, qui consiste à déporter sur des serveurs distants des stockages et des traitements informatiques habituellement localisé sur des serveurs locaux ou sur le poste de l'utilisateur pour être ensuite accessible depuis n'importe où, à la condition d'avoir une connexion Internet.

Grace à l'informatique dans le nuage, les cybercriminels risquent d'exploiter les données qui y sont hébergées en masse et de commettre différents types d'infractions informatiques à distance.

Bref, il ne fait aucun doute que la cybercriminalité s'appuiera largement sur ces technologies émergentes et posera par conséquent de nombreux défis aux services de répression que ce soit en matière d'identification des auteurs des cybercrimes ou de la préparation des preuves.

Pour y faire face, la stratégie de lutte contre la cybercriminalité doit être en mesure d'anticiper ces technologies émergentes afin d'analyser et se préparer à leurs implications sur la cybersécurité.

Les différents types de cybercrimes y compris ceux découlant des technologies émergentes n'épargnent aucune catégorie de victimes potentielles, depuis les particuliers eux-mêmes, utilisateurs d'Internet, jusqu'au monde de l'entreprise et les services de l'Etat.

En ce qui concerne **d'abord** les particuliers, ces derniers, surtout les plus vulnérables ( mineurs…) sont particulièrement visés par les cyberdélinquants : usurpation d'identité, fishing, spaming, cyberharcellement, diffamation, injure, dénigrement, Xénophobie et racisme en ligne, cyberharcellement sexuel…etc.

Pour ce qui est des entreprises **ensuite**, elles sont des cibles privilégiés des cyberpirates surtout leurs systèmes d'information sur lesquelles reposent toutes leurs activités : intrusion, altération, entrave, infection virale, cookies, vol de données sensibles….

S'agissant **enfin** de l'Etat, les systèmes d'information souverains et les infrastructures d'importance vitale peuvent être également la cible  d'attaques cybercriminelles ( cyberterrorisme, cyberespionnage, cyberguerre…) qui portent atteinte à ses intérêts fondamentaux.

La sécurité dans ces domaines sensibles est un enjeu de souveraineté pour l'Etat qui a la responsabilité de garantir la sécurité de ses propres systèmes d'information et la continuité des institutions et des infrastructures jugées vitales pour les activités socio-économiques du pays.

Sur ce chef, il est à indiquer que l'utilisation d'Internet par les réseaux terroristes, en particulier pour communiquer, inciter à la radicalisation, recruter, faire de la propagande au terrorisme, attaquer les sites gouvernementaux ,financer des actes terroristes.., fait peser une grave menace sur la sécurité du pays.

Pour les raisons que voilà, le concept de défense ne pouvait plus se concevoir comme la réponse à une agression classique, mais devait aussi englober d'autres formes de menaces, surtout les attaques informatiques contre les systèmes d'informations sensibles et les infrastructures d'importance vitales eu égard à leur dépendance de plus en plus forte vis à vis de l'informatique et des réseaux.

Dans un contexte nationale et internationale marqué par la monté en puissance des cybercrimes ( cyberdélits, cyberpiratage, cyberattaques, cyberespionage, cyberterrorisme…) il était nécessaire pour le Maroc de mettre en place une stratégie  pour combattre ce fléau.

L'un des éléments déterminants de cette stratégie est relatif à la mise en place d'une législation en cette matière. Cette dernière doit couvrir tous les domaines, notamment l'incrimination, la procédure judiciaire, la responsabilité des prestataires de services Internet et la coopération internationale.

En ce qui concerne l'incrimination, le Maroc dispose aujourd'hui d'outils juridiques dans beaucoup de domaines affectés par la cybercriminalité. L'arsenal juridique se renforcera certainement par la prochaine révision du code pénal et la prochaine promulgation du code numérique.

L'élément juridique ne sera à notre avis pas complet sans l'encadrement juridique de l'activité des prestataires de services Internet.

Ces derniers, qui englobent les prestataires de services techniques ( opérateurs de télécommunications, Fournisseurs d'accès, fournisseurs d'hébergement ), les prestataires de services d'intermédiation ( liens hypertextes, annuaires, moteurs de recherche ) et les fournisseurs de services de connexion alternative ( cybercafés, points de connexion Wifi ), jouent un rôle déterminant dans le fonctionnement de l'espace dans lequel se commettent les cybercrimes à savoir l'Internet.

C'est la raison pour laquelle la mise en place d'un cadre juridique déterminant la responsabilité de chacun de ces prestataires dans les infractions commises sur le réseau internet est indispensable.

Par ailleurs, le même cadre juridique doit prévoir des obligations en matière de conservation des données électroniques de connexion et de leur communication en cas de besoin aux autorités judiciaires pour faciliter l'identification des auteurs des cybercrimes.

D'un autre côté, et eu égard au caractère par essence mondial et sans frontière du cyberespace, la cybercriminalité présente la particularité d'ignorer les frontières étatiques.

Elle est transfrontalière parce que d'abord, les auteurs, complices et victimes peuvent se trouver dans des pays différents, ensuite, les éléments matériels de preuves de certaines infractions peuvent être dispersés sur des territoires différents.

D’où la nécessité d’intégrer la coopération internationale dans toute stratégie de lutte contre la cybercriminalité. Cette dernière  comprend l’extradition, l’entraide judiciaire, la reconnaissance mutuelle des jugements étrangers…etc.

**En guise de conclusion,**

Il va sans dire que le Maroc se heurte aujourd’hui à des difficultés dans l’appréhension de la cybercriminalité et cherche à passer à une seconde étape par la refonte de sa stratégie de lutte.

Pour réussir, cette dernière doit mettre en place une plus grande synergie entre la lutte contre la cybercriminalité, la cyberdéfense et la cybersecurité afin de créer un espace de cyberconfiance nécessaire pour le développement des activités numériques.

**Docteur Fouad BENSEGHIR**

*Expert en Droit Electronique*