Cadre conceptuel et théorique de la cybercriminalité

Par Mr FARIH OMAR

Master " Gestion et Droit des Technologies de l'Information et de Communication dans les deux Rives méditerranéennes"

Faculté des sciences juridiques économiques et sociales de Fès

(Promotion 2010-2012)

Chapitre 1 : Concepts et Généralités sur la Cybercriminalité

Le millénaire actuel reste prédominé par l'apparition des (nouvelles) technologies de l'information et de la communication (NTIC) qui s'avèrent omniprésentes, et dont la tendance à la numérisation va grandissant. Internet en est l'une des infrastructures techniques dont l'explosion et la croissance sont très spectaculaires. La demande de connectivité à Internet et d'interconnexion des systèmes a conduit à l'intégration de l'informatique dans des produits qui, jusqu'alors, en étaient dépourvus.

Malheureusement, toute invention humaine porteuse de progrès peut être aussi génératrice de comportements illicites. Le coté élogieux d'internet occulte la face la plus redoutable ; et parmi les menaces liées à cet outil, une se démarque par sa dangerosité et sa complexité : la cybercriminalité. Celle-ci est l'une des nouvelles formes de criminalité ou de délinquance sur le réseau Internet, dont les conséquences se révèlent être particulièrement graves pour la sécurité humaine. De toute évidence, COLIN ROSE souligne que « la cybercriminalité est la troisième grande menace au monde après les armes chimiques, bactériologiques et nucléaires».

Afin d'appréhender ce phénomène, nous avons divisé le présent chapitre en trois sections suivantes :

Section 1 : la cybercriminalité : concepts et caractéristiques

Section 2 : La cybercriminalité : causes, motivations et conséquences

Section 3 : Les multiples acteurs et visages de la cybercriminalité

Section 1 : la cybercriminalité : concepts et caractéristiques

Le terme de la cybercriminalité a été inventé à la fin des années quatre vingt-dix, alors qu'Internet se répandait en Amérique du Nord[1].

A vrai dire il n'existe pas de définition universelle pour le terme de « cybercriminalité ». Celui-ci est utilisé généralement pour décrire l'activité criminelle dans laquelle le système ou le réseau informatique est une partie essentielle de crime. Il est généralement employé pour décrire des activités criminelles traditionnelles dans lesquelles les ordinateurs ou les réseaux sont utilisé pour réaliser des activités illicites[2].

Le terme donc demeure difficile à conceptualiser car il n'est l'objet d'aucune définition légale, ce choix des législateurs a conduit la doctrine à multiplier les définitions contribuant ainsi à rendre plus complexes les analyses juridiques. De ce fait et pour bien cerner cette notion de cybercriminalité nous allons au début exposer les multiples définitions adoptées par certains pays, et puis mettre le point sur les caractéristiques de ce phénomène pour bien le cerner (2).

1. Définition de la cybercriminalité

1.1.Absence d'une définition légale

La cybercriminalité n'étant pas être définie avec rigueur, elle conduit vers des dérives terminologiques. Ainsi MM.Alterman et Bloch retiennent comme définition du délit informatique, la définition de la cybercriminalité par des

[1]Un sou groupe de pays G8 fut formé suite à une réunion en France, afin d'étudier de nouveau types de criminalité encouragé par ou migrant vers Internet. Ce « groupe de Lyon » employait alors « cybercriminalité » pour décrire, de manière relativement vague, tous les types de délits perpétrés sur internet ou les nouveaux réseaux de télécommunication.

2 ELAZZOUZI. A, « La Cybercriminalité au Maroc », P 18. BISHOPS SOLUTION 2010

experts de l'Organisation pour la Coopération et le Développement économique (OCDE) à savoir : « *tout comportement illégal ou contraire à l'éthique ou non autorisé, qui concerne un traitement automatique de donnée et/ou de transmission de données* ».

En Europe Aucun texte législatif ou réglementaire ne définit la cybercriminalité. Toutefois, certaines notions proches, telles que la criminalité informatique, l'infraction informatique, le délit informatique ou l'usage abusif de l'informatique, ont fait l'objet de définitions posant la question de l'assimilation ou de la distinction du crime et de la cybercriminalité.

Selon le ministère de l'Intérieur français, la cybercriminalité recouvre « *l'ensemble des infractions pénales susceptibles de se commettre sur les réseaux de télécommunications en général et plus particulièrement sur les réseaux partageant le protocole TCP-IP19, appelés communément l'Internet*»

Pour l'Office fédéral de la police suisse, la cybercriminalité s'entend « des nouvelles formes de criminalité spécifiquement liées aux technologies modernes de *l'information, et de délits connus qui sont commis à l'aide de l'informatique plutôt qu'avec les moyens conventionnels* »

Enfin, le Collège canadien de police définit la cybercriminalité comme « *la criminalité ayant l'ordinateur pour objet ou pour instrument de perpétration principale* ».

Cependant, ces définitions ne sont pas complètement définitives : la définition adoptée par le ministère de l'Intérieur français vise seulement les infractions dirigées contre les réseaux de télécommunications. Elle ne recouvre ni les infractions susceptibles d'être commises sur les systèmes informatiques, ni les infractions directement générées par le fonctionnement des réseaux informatiques.

Pour les deux dernières définitions considérées par l'Office fédéral de la police suisse, et le Collège canadien de police utilisent des termes très larges qui

peuvent recouvrir la cybercriminalité, et la criminalité informatique en même temps. Ces confusions nous on conduits à nous interroger sur quelques définitions adoptées aux Etats-Unis.

Aux Etats-Unis, la cybercriminalité forme une grande proportion des délits examinés par la police .Son concept diffère d'un Etat à l'autre, et d'un département de police à l'autre. Selon le Département de la justice (*United States Department of Justice*) la cybercriminalité est considérée comme « *une violation du droit pénal impliquant la connaissance de la technologie de l'information pour sa perpétration, son investigation, ou ses procédures pénales* ».

De son coté, le Code pénal de Californie (section 502), définit une liste d'actes illicites qui tombent sous le coup de la cybercriminalité. Il considère comme cybercriminalité le fait « *d'accéder, ou de permettre intentionnellement l'accès, à tout système ou réseau informatique afin a) de concevoir ou réaliser tout plan ou artifice pour frauder ou extorquer ; b) d'acquérir de l'argent, des biens, ou des services, dans le but de frauder ; c) d'altérer, de détruire, ou d'endommager tout système, réseau, programme, ou données informatiques* »[3].

1.2. La cybercriminalité : définition pratique

La cybercriminalité peut être définie comme : toute action illicite associée à l'interconnexion des systèmes informatiques et des réseaux de télécommunication, où l'absence de cette interconnexion empêche la perpétration de cette action illicite[4].

Sous cette définition, nous pouvons identifier les quatre rôles que joue le système informatique dans les actes illicites :

Objet : Des cas concernant la destruction de systèmes informatiques, ainsi que des données ou des programmes qu'ils contenaient, ou encore la destruction

[3] Code pénal de l'Etat de Californie (section 502).
[4] CHAWKI.M, « Essai sur la notion de cybercriminalité", p23, IEHEI, juillet 2006

d'appareils fournissant l'air climatisé, l'électricité, permettant aux ordinateurs de fonctionner.

Support : Un système informatique peut être le lieu ou le support d'une infraction, ou un ordinateur peut être la source ou la raison d'être de certaines formes et sortes d'avoirs qui peuvent être manipulés sans autorisation.

Outil : Certains types et certaines méthodes d'infraction sont complexes pour nécessiter l'utilisation d'un système informatique comme instrument. Un système informatique peut être utilisé de manière active comme dans le balayage automatique de codes téléphonique afin de déterminer les bonnes combinaisons qui peuvent être utilisées plus tard pour se servir du système téléphonique sans autorisation.

Symbole : Un système informatique peut être utilisé comme symbole pour menacer ou tromper. Comme, par exemple, une publicité mensongère de services non existants, comme cela a été fait par plusieurs clubs de rencontres informatisés.

2. Les caractéristiques de la cybercriminalité

Certes, la cybercriminalité est l'une des nouvelles formes de criminalité ou de délinquance sur le réseau Internet, dont les conséquences se révèlent être particulièrement graves pour la sécurité humaine. La dangerosité de ce phénomène est due à son caractère mondial d'un coté, et d'un autre coté de l'organisation de ses acteurs, leur spécialisation… on parle ainsi d'une économie souterraine d'une criminalité mondialisée et en même temps mondialisée.

2-1. La cybercriminalité : une délinquance organisée

A l'origine conçue comme une succession de défis à la sécurité des réseaux, la cybercriminalité se teinte désormais d'une coloration mafieuse, donnant naissance à de véritable « *marchés noirs* » d'information piratée, allant des atteintes à l'identité à la propriété intellectuelle et artistique, aux fraudes à la carte bancaire. Désormais, il existe des liens étroits entre la criminalité classique

et la criminalité informatique. En outre, les cybercriminel font de plus en plus partie de réseaux internationaux très organisé.

2-1-1. Typologie de cyberdélinquants

Si la vengeance ou le désir d'exister sont des motivations fréquentes chez les délinquants du net, le principal moteur reste l'appât du gain. Le milieu des délinquants du net est désormais souvent très bien organisé et structuré en fonction de leurs tâches, de leur niveau de connaissance et de leurs cibles. Certains jeunes ayant souvent un comportement relevant de l'addiction à l'internet, agissant encore de façon isolée comme ce fameux « *Hacker croll* » récemment interpellé et jugé après avoir piraté en 2009 des comptes Twitter notamment celui de Président ***Barak Obama***[5]**.** L'homme était connu de force de police pour une escroquerie en ligne qui lui aurait rapporté 15000 euros. Il a été condamné à 5 mois d'emprisonnement avec sursis, les réquisitions du parquet étant dépassés de trois mois. Il est à noter qu'il y a encore trop souvent une certaine bienveillance accordé à ces pirates, la cybercriminalité étant encore parfois prise à tord comme une sorte de défi ludique.

Certains fabriquent de logiciels malveillants, tandis que d'autres les utilisent ensuite afin de perpétrer des actions criminelles. Il est difficile de dresser une typologie de cybercriminalité. On observe aujourd'hui des mafias organisés qui s'étendent dans les pays de l'Est ou d'Amérique du Sud avec une hiérarchie organisée de plusieurs strates qui communiquent entre elles, la base étant constituée par celle des codeurs-programmeurs. Par exemple, un kit de phishing s'achète de 20 dollars et la mise en place d'une opération de phishing coute 60 dollars. La rentabilité de cette opération est donc immédiate, même s'il faut faire des campagnes à quelques millions de *spams*. Le cybercrime est devenu une industrie, avec ses fournisseurs de services, ses virus clés-en main, ses entreprises innovantes, ses intermédiaires, ses architectes de système, ses

[5] http://www.01net.com/editorial/514625/comment-hacker-croll-a-pirate-des-comptes-twitter/ consulté le 21/05/2012

fournisseurs de fichiers de coordonnées bancaires ou d'adresse mail. Ce constat est très visible dans certains pays de l'ancien bloc de l'Est comme la Roumanie, l'Ukraine ainsi qu'en Russie[6]. (Voir tableau page suivante)

Script kiddles	Jeunes de 15 à 20 ans qui constitue la « main d'œuvre »
Drops	Transforme l'argent virtuel en argent réel
Mules	Intermédiaires prêtant ses comptes aux cyberdéliquants
Crackers (black hat)	Pénètre les réseaux avec intention de nuire
Hackers	Pirates informatique. Criminalité organisé, mafias
Spammeurs	Etudiant ou cadre informatique cherchant une source de revenu supplémentaire

Tableau 1 *: Différents types de cyberdélinquants*[7]

2-1-2. La cybercriminalité : Une économie souterraine

Les données recueillies par les pirates peuvent être vendues sur des marchés clandestins, spécialisés dans ce genre de transactions. Le prix pratiqué pour l'envoi de 10 millions de *spams* par jour se situait aux environs de 600 dollars en 2007. Un numéro de carte de crédit sans PIN, mais avec les donnés requises pour réaliser des opérations d'e-commerce se négociait 25 dollars, un numéro de carte de crédit avec le PIN correspondant revenait à 500 dollars. Selon leur type, les cheveux de Troie peuvent être acquis à des prix allant de quelques centaines à plusieurs milliers de dollars.

Les informations se vendent aujourd'hui de moins en moins cher, signent qu'elles sont plus faciles à voler, et à trouver, les pirates tant protégés d'une part

[6] QUEMENER. M, Y.CHARPENEL. Y, « Cybercriminalité Droit pénal appliqué » ,P 12,13. Edition Economica, 2010.
[7] Idem

par l'utilisation de pseudonymes et d'autre part par le nombre croissant. On parle de véritables réseaux « *undeground* », développés en Europe et de l'Est, mais aussi aux Etats-Unis, en chine, et en Allemagne.

2-2. La cybercriminalité : une criminalité mondialisée

la cybercriminalité est l'une des formes de délinquance qui connait actuellement la croissance la plus forte, de plus en plus de malfaiteurs exploitant la rapidité et la fonctionnalité des technologies modernes, ainsi que l'anonymat qu'elles permettent, pour commettre les infractions comme le piratage des données et des systèmes informatiques, le vol d'identité, la diffusion d'images de pédopornographie, ou les escroqueries sur internet, etc.

2-2-1. Caractère planétaire de la cybercriminalité

Mondial par nature, Internet permet aux délinquants de se livrer à presque n'importe quelle activité illicite au plan international. Il est donc essentiel que tous les pays fassent évoluer leurs moyens de lutte sur le plan national de façon à ce que les infractions commises dans le cyberespace ne demeurent pas hors d'atteinte. L'utilisation d'Internet par des terroristes, en particulier pour inciter à la radicalisation et pour recruter, fait peser une grave menace sur la sécurité, tant au niveau national qu'international.

La particularité de la délinquance des réseaux numériques est qu'elle a pour cible un territoire désormais sans frontière et mondialisé. Les cyberdélinquants vont par exemple commettre des attaques dans un pays où la législation est encore inexistante et les effets de leurs actions vont se faire sentir à l'autre bout du monde, ce qui rend souvent très complexe le déroulement des enquêtes[8].

Section 2 : La cybercriminalité : causes, motivations et conséquences

[8] QUEMENER. M, CHARPENEL. Y. « Cybercriminalité Droit pénal appliqué », op.cit P 14.

Pour bien cerner la notion de la cybercriminalité, il est important de s'attarder aux multiples causes qui ont contribué à l'expansion spectaculaire des cas de cybercrimes, sans bien sur oublier les enjeux et les motivations de cybercriminalité et enfin mettre l'accent sur les conséquences de ce phénomène

1. La cybercriminalité : phénomène à multiples causes

L'expansion du phénomène de la cybercriminalité n'est pas venue du hasard, plusieurs facteurs et causes s'y participent à savoir : l'internet d'un coté et les maillons faibles de la sécurité informatique

1-1. L'Internet : le nouveau filon des organisations cybercriminelles

Selon un spécialiste de la cybercriminalité « *Les braquages des fourgons blindés existeront toujours mais on ne pas en faire plusieurs dans la journée ou dans la semaine! Dans le cas des attaques informatiques, c'est possible : on peut automatiser des opérations quotidiennes. Et en plus le coût (en terme de moyens nécessaires à l'attaque et de risques juridique et physiques) est moins élevé* … ». Pour ce spécialiste très au fait de la cybercriminalité, l'avenir apparait donc comme une évidence : les hold-up virtuel vont augmenter[9].

C'est pour cela qu'en 2005 et c'est pour la première fois que le montant des vols générés sur Internet soit supérieur à celui du trafic réel. Selon les estimations des chercheurs de l'organisation *Comuter Economics*, en 2004, le montant des pertes engendrées par ces différentes attaques était de presque 18 milliard de dollars.

Alors la cybercriminalité a trouvé dans le net un espace adéquat pour se développer. En effet grâce notamment à la diffusion sur le web de nouveaux services et outils s'adressant à une population mondiale de plus en plus adoptée à les adopter , la croissance des actes cybercriminels s'est particulièrement accélérée ces trois dernières années. Cette tendance s'amplifie rapidement

[9] Filiol. E, RICHARD. P. « Cybercriminalité enquêtes sur les mafias qui envahissent le Web ». P1 ». Duond, Paris, 2006

depuis la vogue du Web 2.0, notamment les réseaux sociaux qui ont atteint un niveau de popularité élevé parmi les sites web. Ils sont devenus des vecteurs privilégiés de propagation de programmes malveillants et de courriers indésirables. L'efficacité d'une telle diffusion est d'environ 10%. Ce qui est bien supérieur à l'efficacité des méthodes classiques de diffusion des programmes malveillants par courrier électroniques[10].

Autres les réseaux sociaux, les nouveaux services afférents aux blogs, aux forums, à Twitter, etc.… sont à l'origine de la croissance d'attaques. En effet, tous ces services en ligne jouent sur la confiance établie entre les membres d'un même réseau, la facilité de téléchargement, de publication et d'autres techniques d'échanges des informations, qui rendent leurs utilisateurs vulnérables aux infections de logiciels malveillants. Ces nouveaux services ont donné une ampleur sans précédent à certaines formes de fraude, qui se sont particulièrement épanouies sur l'internet[11].

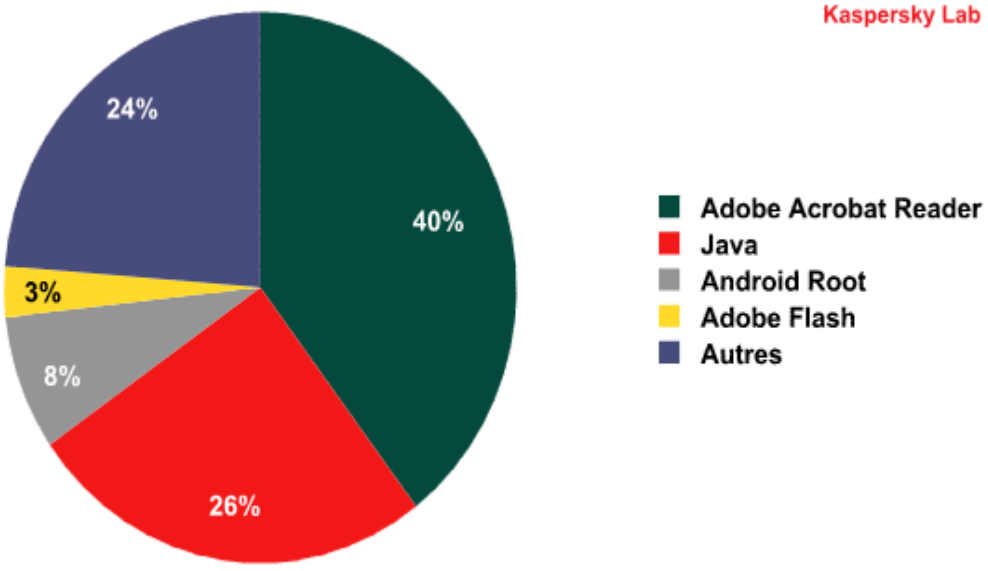

Schéma 1: ***Applications dont les vulnérabilités ont été exploitées par des codes d'exploitation Internet Premier trimestre 2012***[12]

[10] Baromètre annuel sur la cybercriminalité en 2008 par Kaspersky lab.
[11] ELAZZOUZI. A, la cybercriminalité au Maroc. P18.Bischops Solution. Juin 2010
[12] http://www.viruslist.com/fr/analysis?pubid=200676286 consulté le 12/06/2012

Les vulnérabilités CVE-2011-3544 dans Java est exploité dans près d'un quart des attaques. Cette vulnérabilité a été une des favorites des individus malintentionnés tout au long du trimestre : elle a été utilisée pour diffuser le bot Hlux, le cheval de Troie Carberp ainsi qu'un bot dématérialisé

1-2. Les maillons faibles de la sécurité informatique

En matière de sécurité, quel que soit le domaine considéré, la cause des problèmes relève toujours de deux aspects qui peuvent intervenir séparément ou simultanément :

- Une erreur, volontaire ou non de l'utilisateur
- Un défaut dans le système concerné, soit au niveau de l'outil lui-même, soit au niveau de la fonctionnalité mise en œuvre par cet outil (le protocole).

Pour illustrer ce constat, prenons un exemple de la vie quotidienne, celui de la conduite automobile. Quelles peuvent être les causes d'un accident ?

- Une mauvaise « conduite » du conducteur, provoquée par l'environnement, par une tendance naturelle (laxisme, indiscipline…) ou par des contraintes diverses telles le manque de temps ;
- Un défaut d'entretien du véhicule (assimilable au système informatique) ;
- Le mauvais état ou la mauvaise conception des routes et de la signalisation (assimilable au protocole).

Il est intéressant de remarquer que ces trois causes sont classées par ordre décroissant de probabilité de réalisation, les accidents étant souvent engendrés par la faute directe des usagers que par le mauvais état des routes. Cet exemple s'applique parfaitement au domaine de la sécurité informatique et les causes d'accidents sur nos routes sont transposables sur les « autoroutes de l'informations ».

Un mauvais comportement de la part de l'internaute a toujours deux causes possibles :

- Ses dispositions « naturelles » au laxisme et à la facilité qui entre plusieurs alternatives, lui font souvent choisir le moindre effort ;

- Son attirance tout aussi « naturelle » pour certaines choses (pornographie, jeux, sport…).

Mais ces comportements ne sont mauvais dans l'absolu que parce qu'il existe **un autre acteur** important dans tout attaque : le pirate, le hacker, l'escroc… Bref, celui que nous nommerons le malfaisant informatique. Pour atteindre sa cible, il va déployer une stratégie très efficace : mettre à son profit les mauvaises habitudes des usagers pour les transformer en comportement dangereux pour la sécurité informatique. C'est ce que l'on appelle « *l'ingénierie sociale* »[13].

L'ingénierie sociale

Parmi les nombreuses définitions , plus au moins précis, de l'expression « ingénierie sociale » nous adopterons la suivante : « *ensemble des techniques de manipulations psychologiques ou d'exploitation comportementale d'un individu, ou d'un groupe d'individus, par des personnes malfaisants dont le but est l'incitation inconsciente à amoindrir, contourner ou supprimer les mesures de sécurité d'un système par ce ou ces individus*[14] ».

Sachant bien que la sécurité des systèmes d'informations repose sur les trois piliers suivants :

- *La confidentialité* : les informations ne doivent être accessibles qu'aux seules personnes autorisées ou habilitées. Un mot de passe ou un code de carte bancaire sont les meilleurs exemples d'informations confidentielles.
- *L'intégrité* : les informations (un fichier système par exemple) ne doivent être modifiées que par une action légitime et volontaire.
- La disponibilité : le système doit répondre aux sollicitations des utilisateurs autorisés (accès aux informations, action particulière…) dans le

[13]Filiol. E, « l'ingénierie sociale ». Linux Magazine 42, 2002
[14] Filiol.E, Richard.P « CYBERCRIMINALITE enquête sur les mafias qui envahissent le WEB » p 14.Imprimerie nouvelle, 2006

délai imparti par le cahier de charges, propre à chaque application et/ou système.

L'attaquant a alors deux axes d'approche pour tenter de porter atteinte à la sécurité du système considéré : soit il en vise directement les éléments techniques (exploitation de failles, de la mauvaise gestion, de mauvaises configurations ...), soit il s'attaque directement à l'utilisateur ou à l'administrateur pour l'amener à effectuer certaines actions lui permettant de porter atteinte au système. En clair, le pirate peut soit exploiter un « bug » déjà présent, soit transformer l'élément humain lui-même en un « bug ». Dernière alternative : utiliser les travers de l'utilisateur pour le transformer en « code malveillant ».

L'attaquant dispose de plusieurs moyens pour modifier le comportement de l'utilisateur :

- *L'usurpation d'identité* : le but est de se faire passer de l'utilisateur cible pour une personne ou une entité connue et /ou identifiée comme appartenant bien à un groupe autorisé et dépositaire d'une légitimité certaine dans la politique de sécurité de l'organisme ou auprès de l'utilisateur. C'est l'une des techniques utilisé lors de l'attaque ***phishing***[15] **:**

L'internaute reçoit un e-mail venant soi-disant de sa banque qui lui demande –sous le prétexte d'une mise à jour de sécurité[16] – de cliquer sur un lien Internet pour redonner son identifiant et son mot de passe. Dans ce premier cas, il y a toujours défaut d'identification et/ ou d'authentification. Le résultat est, au minimum, une atteinte à tout ou partie de la confidentialité de système.

[15] Voir chapitre 1 : section 3

[16] Les banques et autres organismes financiers ne se sont pas les seules victimes de l'usurpation. Il y a aussi Microsoft. Des pirates ont en effet envoyé des e-mails provenant soit disant de cet éditeur. Sous un prétexte de mise à jour logicielle, ils demandaient aux internautes d'ouvrir la pièce jointe ou de cliquer sur un lien URL. Evidement le colis était piégé et contenait un virus ou un cheval de Troie.

- *La manipulation psychologique* : il s'agit d'exploiter diverses « faiblesse » ou « tendances » psychologiques de la victime en particulier et/ou humaines en général : manque d'affection, bons sentiments, ego, appât de gain faciles, manque de bon sens, de perspicacité, de prudence, laxisme, manque de conscience professionnelle.

- *L'exploitation du manque de connaissance* : la méconnaissance technique de la plupart des utilisateurs, voire de certains administrateurs, le manque de formation continue (veille technologique), de sensibilisation régulière sont directement exploités par l'attaquant[17] pour parvenir à ses fins. Bien souvent la crédulité des utilisateurs amplifie les choses. L'utilisation de canulars (hoax en anglais) est l'un des moyens les plus connus.

En résumé la sécurité n'est pas seulement un enjeu technologique. autrement dit, pour assurer la sécurité d'un système d'information on se limite pas à la mise en place d'un pare feu et d'un antivirus car ces dispositifs ne sont pas d'une grande utilité quand il s'agit par exemple d'attaque type « ingénierie sociale » qui connait ces dernière années une évolution spectaculaire[18]. L'exemple est celui des organisations CIA, FBI et le Pentagone qui ont fait l'objet d'attaque malgré qu'elles disposent de moyens colossaux pour assurer un niveau de sécurité adéquat. Résultat : c'est la dimension organisationnelle voir humaine qui est souvent négligée.

2. La cybercriminalité : activité attractante mais très préjudiciable

L'attractivité du phénomène de cybercriminalité est due à sa facilité, sa rentabilité et à son faible risque. Tous ses facteurs motivent les milliers d'internautes à franchir leur premier pas dans ce monde de fraudes informatiques, d'escroqueries et de piratages… toutes ces activités

[17] Trois types d'attaquants : il peut s'agir d'un simple pirate qui inspiré par la bêtise, une volonté de nuisance ou l'appât de gain. Autre profil : des groupes très bien organisés, d'inspiration mafieuse ou étatique étrangère. Il y a enfin des sociétés spécialisées dans le renseignement ou la guerre économique qui agissent le plus souvent pour des sociétés concurrentes de celles attaquées.

[18] ELAZZOUZI. A, « la cybercriminalité au Maroc ».p22.Bishops Solution. Juin 2010

cybercriminelles génèrent à leurs auteurs des milliards d'argent mais coutent chère soit aux organisations soit à l'économie étatique.

2-1. La cybercriminalité : activité facile, rentable et à faible risque

La cybercriminalité est une activité facile : avec la vulgarisation des modes opératoires cybercriminels sur l'internet, aujourd'hui il n'est pas nécessaire de disposer de compétences techniques pour lancer une opération cybercriminelle ; le niveau d'expertise technique requis pour un projet cybercriminel n'a plus du sens du moment ou il est possible aujourd'hui d'acheter librement des logiciels espions les plus élaborés ainsi que les données collectées par ces mêmes logiciels : informations bancaires et informations personnelles suffisantes pour acheter en ligne ou transférer des fonds. En outre, il est aussi possible de commander un acte cybercriminel ponctuellement auprès de prestataires spécialisés qui viennent chacun apporter leur part d'expertises dans l'opération, chaque maillon générant des bénéfices dont le montant répond uniquement aux lois de l'offre et de la demande, la rareté d'une compétence augmentant les prix en conséquence.

Il existe de nombreuses ressources disponibles permettant de mettre au point des solutions complètes. Ces solutions vont de l'usage de la simple vulnérabilité, jusqu'à l'emploi des chevaux de Troie permettant d'automatiser des réseaux ou « *botnets*[19] ».

[19] Un botnet est un réseau d'ordinateur Zombies contrôlés à l'insu de leurs propriétaires.

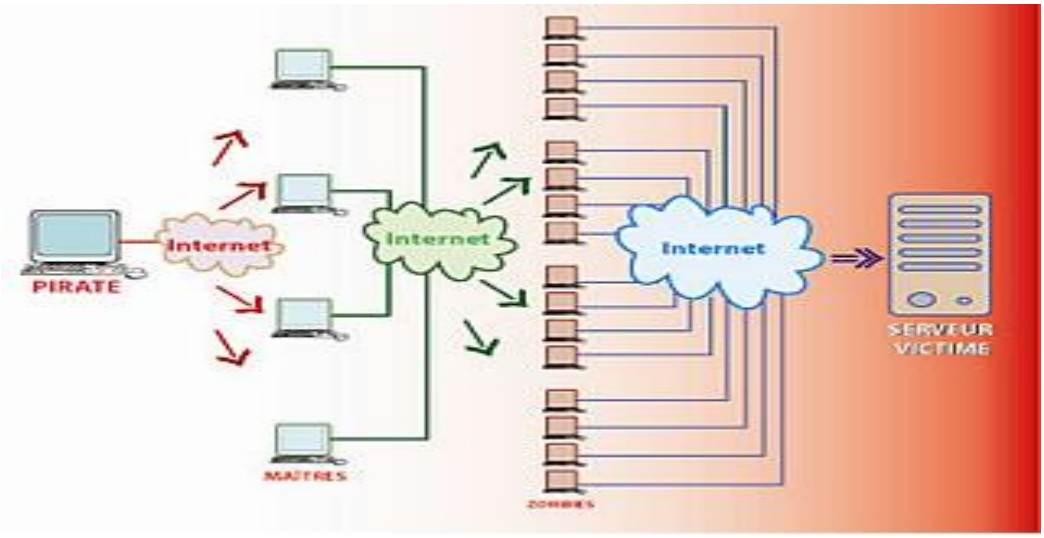

Schéma 2 : *Création et utilisation d'un Botnet*[20]

La cybercriminalité est une activité rentable : Le crime contemporain est un métier comme un autre. La cybercriminalité est une forme d'exploitation économique qui répond aux mêmes critères de gestion traditionnels, tels que la rentabilité ou la gestion des risques, la facilité d'utilisation des produits ou l'importance des marchés émergents.

Le critère le plus important pour n'importe quelle entreprise étant la rentabilité, la cybercriminalité ne fait pas exception à la règle. C'est un fait que la cybercriminalité est extrêmement profitable. De grandes sommes ont été volées avec succès, tantôt en une seule fois, tantôt par petites quantités mais en très grand nombre[21].

La cybercriminalité a couté en 1.000 milliards de dollars d'après une étude de Mcafee présentée au forum de Davos.

Rien qu'en 2007, par exemple, chaque mois, des actions cybercriminelles d'envergure étaient commises :

20 GERCKE. M, Comprendre la cybercriminalité: Guide pour les pays en développement, 2009.

[21] http://www.viruslist.com/fr/analysis?pubid=200676168 consulté le 31/05/2012

Tableau 2 : *Célèbres actions cybercriminels de l'année 2007*[22]

Janvier 2007	Des pirates russes, avec l'aide d'intermédiaires suédois, auraient détourné 800 000 euros de la banque suédoise Nordea
Février 2007	La police brésilienne arrête 41 pirates pour avoir utilisé un cheval de Troie pour voler les accès à des comptes bancaires et détourner 4,74 millions de dollars.
Mars 2007	Cinq ressortissants d'Europe de l'Est sont emprisonnés au Royaume Uni pour une fraude à la carte bancaire ; ils auraient dérobé 1,7 millions de livres.
Jin 2007	150 cybercriminels sont arrêtés en Italie ; ils sont accusés d'avoir bombardé des utilisateurs italiens avec des faux messages, qui leur auraient rapporté 1,25 millions d'euro sous forme de gains frauduleux.
Juillet 2007	Des cyber-délinquants russes sont accusés d'avoir utilisé un cheval de Troie pour voler 500 000 dollars dans des banques de Turquie.
Août 2007	L'ukrainien Maxim Yastremsky (alias « Maksik ») est arrêté en Turquie, accusé d'avoir empoché dix millions de dollars après le vol d'identificateurs.
Septembre 2007	Gregory Kopiloff est condamné aux États-Unis pour avoir utilisé les logiciels de partage de fichiers (P2P) Limewire et Soulseek pour collecter des données qu'il employait pour des usurpations d'identité ; il aurait gagné des milliers de dollars par la commercialisation de données volées
Octobre 2007	Greg King est arrêté aux États-Unis pour avoir participé en février 2007 à une attaque DDoS sur la société Castle Cops ; il affronte une peine maximum de 10 ans de prison et 250 000 dollars d'amendes.
Novembre 2007	Le FBI arrête huit personnes dans la deuxième phase de son opération anti-botnets « Operation Bot Roast », évitant des pertes économiques chiffrées à plus de 20 millions de dollars, et concernant plus d'un million d'ordinateurs pris comme victimes.

La cybercriminalité est une activité facile et à faible risque : un autre facteur essentiel dans la croissance de la cybercriminalité, entendue comme une activité commerciale, est le degré minimum de risques, comparé aux chances de réussite. Dans le monde réel, la dimension psychologique avec la prise de risques réels du crime assurent un certain effet de dissuasion. Mais dans le monde virtuel, les criminels ne sont jamais directement en contact avec leurs victimes ni avec les différentes sociétés qu'ils décident d'attaquer. Il est

[22] Conception personnelle du tableau

beaucoup plus facile de voler des riches ou quelqu'un que vous ne pouvez ni voir, ni toucher ni même connaître.

2-2. Cout et évaluation de la cybercriminalité

Les conséquences financières du cybercrime ont toujours été difficiles à évaluer ; les chiffres sont souvent contradictoires et les sources hétérogène, voire partisanes comme parfois celles des éditeurs de sécurité.

Plusieurs raisons expliquent cette incapacité à mesurer le cout du préjudice de la criminalité informatique, la figure suivante montre quelques unes : (voir page suivante)

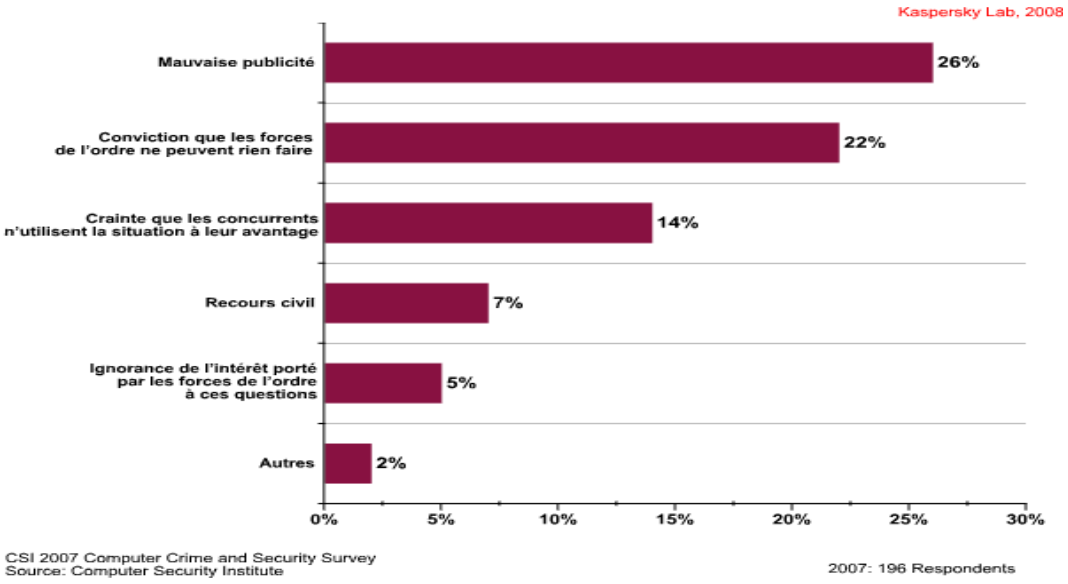

Figure1 : *Raisons avancées par les organismes pour ne pas informer des effractions de sécurité*[23]

Selon cette figure les Causes rendant difficile l'évaluation de la cybercriminalité sont : Le manque des réactions des sociétés ou des particuliers qui tient au fait, souvent, qu'ils ne s'aperçoivent même pas des attaques dont ils

[23] http://www.viruslist.com/fr/analysis?pubid=200676168 consulté le 10/6/2012

sont victimes, la réticence des entreprises de dénoncer ces délits de peur de dévoiler des secrets inhérents à leur systèmes informatiques. Et aussi L'absence d'obligation pour les victimes de porter plaintes.

Depuis l'an 2000, les attaques de sécurité des entreprises dans le monde auraient couté en temps perdu 1600 milliards de dollars, selon le sondage annuel réalisé par Information Week Research., en coopération avec le cabinet de conseil Price Waterhouse Cooper. Au total, les entreprises auraient ainsi gaspillé près de 3,3% de leur temps entre le chômage technique et la répartition des systèmes impactés. D'après la firme Reality Research and Consulting qui a apporté son assistance dans la réalisation de l'enquête, les sociétés du seul continent nord-américain auraient globalement retranché de leur productivité 6822 personnes pendant 365 jours. Alors qu'en 1998, la moitié des entreprises avaient été touchées, le taux serait aujourd'hui passé à près de 74%.

La cybercriminalité a causé un préjudice estimé à 1000 milliards de dollars en 2008, par le vol de données informatiques aux entreprises selon une étude de la société spécialisée dans la sécurité informatique McAfee. Pour cette première étude au niveau international sur « la sécurité des économies de l'information » présentée au Forum économique mondial de Davos (Suisse) des éléments ont été recueillis auprès de plus de800 responsables au Japon, en chine, en Inde, au Brésil, en Grande-Bretagne, à Dubaï, en Allemagne et aux Etats-Unis ce qui lui donne une représentativité certaine.

On peut accorder plus de confiance au bilan annuel du FBI mené en partenariat avec l'iC3 (Crime Complet Center). Ses conclusions sont sans appel.

Selon cette analyse, le cybcercrime aurait couté en 2009 559,7 millions de dollars à l'économie américaine, à savoir deux fois plus que l'année précédente (264,6 millions)[24].

[24] QUEMENER. M, CHARPENEL. Y, « CYBERCRIMINALITE droit pénal appliqué ». P 10, 11. Ed ECONOMICA 2010.

Section 3 : Les multiples auteurs et visages de la cybercriminalité

Chaque acte cybercriminel suppose l'interaction entre plusieurs acteurs aux aspirations diverses. Il ne peut être la résultante d'une action perpétrée par un seul individu. Mener à bien une opération cybercriminelle, ayant notamment comme objectif l'appât de gain, repose inévitablement sur une logique de spécialisation, de division de travail et de répartition des tâches. Une telle logique est nécessaire pour la formation d'un écosystème cybercriminel dont son univers *Underground,* qui est sa composante majeure, demeure difficilement pénétrable. Dans ce cadre est pour bien éclaircir les choses nous allons dans un premier temps lister les différents acteurs de l'univers Underground (1) et après nous métrerons en exergue les multiples visages de cybercriminalité causée par ces acteurs (2).

1. Les auteurs de l'univers Underground

Contrairement à ce qu'anime souvent notre imaginaire collectif, le pirate n'est qu'un maillon de la longue chaîne constituant l'univers *Underground*. Ce dernier se compose d'une multitude d'acteurs aux aspirations différentes. Mais ce qui est remarqué c'est que la classification de ces auteurs est presque impossible car les frontières entre eux sont de plus en plus floues.

1-1. Le Hacker

Les sens donnés au terme de hacker sont très variés. A la base, un hacker est une personne qui a du plaisir à explorer en détail un système programmable et qui cherche à étendre au maximum ses connaissances dans ce domaine. Actuellement, le terme est, généralement, employé pour désigner des personnes s'introduisant illégalement dans de systèmes informatiques[25].

[25] En France, un hacker avait trouvé le moyen de reprogrammer à distance les taux de change d'un distributeur de billets. Il s'octroyait, par exemple, un taux de change de 5 dollars pour 1 franc. Il effectuait l'opération inverse, le taux de change passait à 5 francs pour 1 dollar et il retournait changer ses Dollars et recevait ainsi 2500 Francs.

Beaucoup de hackers explorent les systèmes informatiques par simple curiosité et par défi intellectuel. Les « vrais » hackers ont un code éthique leur interdisant la destruction de toute information[26], se sont qui ont choisi la voie de la « sagesse « en évitant de déployer leur compétence pour nuire. Nous parlerons dans ce cas de « ***white hat hacker*** ».

1-2. Les black hat hacker

C'est-à-dire des personnes s'introduisant dans les systèmes informatiques à des fins malveillantes. Ils peuvent détruire ou dérober des données, attaquer d'autres systèmes, ou effectuer tout autre acte nuisible. Rappelons par ailleurs que si à l'origine le hacker qui pénètre par effraction dans des systèmes ou des réseaux avait un objectif personnel, aujourd'hui derrière ces actes malveillant, il y l'appât de gain.

1-3. Les « scripts kiddies »

L'expression *Script Kiddie* (traduction littérale « adolescent du scriipt) n'est en vogue que depuis quelques années. Les « *scripts kiddies* » sont des jeunes utilisateurs du réseau utilisant des programmes trouvés sur l'internet, généralement de façon maladroite, pour vandaliser des systèmes informatiques a fin de s'amuser. Souvent peu compétent, ils se contentent d'utiliser des outils d'exploitation automatique à la recherche souvent aléatoire de machines potentiellement aléatoires.

Malgré leur niveau de qualification faible, les *scripts Kiddies* sont parfois une menace réelle pour la sécurité des systèmes. En effet, autre le fait qu'ils peuvent par incompétence altérer quelque chose sans le vouloir ou le savoir, d'une part les *script kiddies* sont très nombreux, et d'autre part ils sont souvent obstinés au point de passer parfois plusieurs jours à essayer toutes les

[26] RMAlL. B, « Criminalité informatique ou liée aux nouvelles technologies de l'information et de la communication ». P 104, 105. SOMAGRAM, 2ém édition, 2010

combinaisons possibles d'un mot de passe, avec le risque d'y parvenir bien que souvent, c'est le *script kiddie* lui-même qui se fait infecter[27].

1-4. Les phreakers

Le mot anglais *phreaking*[28] est obtenu par la contraction de phone et freak, le terme freak signifiant « marginal », ou personne appartenant à une contre-culture. Le pirate téléphonique est appelé un *phreaker*. Donc le phreaking, est l'action de pirater les réseaux téléphoniques. Cette activité est liée au piratage informatique parce que les hackers devaient passer de longues heures à essayer de se connecter par modem, sur les ordinateurs qu'ils avaient pris pour cible et que cela aurait fini par leur coûter cher. C'est pour cela que la plupart des hackers sont aussi des *phreakers*. En outre, comme les centraux téléphoniques modernes sont des ordinateurs, le piratage du téléphone se rapproche beaucoup de piratage d'un ordinateur classique.

1-5. Les carders

Les *carders* s'attaquent principalement au système de cartes bancaires pour en comprendre le fonctionnement et en exploiter les failles. Le terme carding désigne le piratage de cartes bancaires.

1-6. Les crackers

Le cracker est un individu qui enfreint la sécurité d'un système, terme créé vers 1985 par des hackers en réaction à l'usage impropre que faisaient les journalistes du mot hacker.

Le hacking et le cracking se ressemblent beaucoup moins qu'on ne le pense.les crackers ont tendance à se rassembler en petit groupe unis et très secrets ; ce comportement n'a pas grand-chose à voir avec le pluralisme culturel revendiqué par les hackers.

[27] http : // fr.wikepedia.org/wiki/Script.kiddie

28 Le premier cas de phreaking découvert remonte à 1961 et le premier article sur ce sujet fut écrit en 1971 dans le magazine Esuire.

Il est important de signaler qu'il ya autre définition de terme *crakcer* : il ya quelques années, la plupart des éditeurs logiciel de système de protection contre la copie pour tenter d'empêcher le piratage de leurs programmes. Ces systèmes ont été exploités entre 1980 et 1985, beaucoup plus tard dasn certains cas. Comme toujours avec ce genre de système, un moyen de contourner le mécanisme de protection a fini par être découvert et les copies ont inondé le marché. Les personnes capables de « cracker » les mécanismes de prtotection contre la copie ont été baptisé crackers.

Le seul point entre les crackers de système de protection contre la copie et les crackers contemporains est l'éventuelle illégalité de leurs activités. Dans le passé, enfreindre les systèmes de protection contre les copies ne constituait peut être pas un acte illégal en soi, mais la distribution des copies l'était bel et bien[29].

Au Maroc, plusieurs cas de cracking ont été découvert : en juin 2006 un groupe de crackers marocains se faisant appeler "*Team Evil - Reason for Hate*" a fracturé et endommagé plus de 750 sites israélien. Selon des ingénieurs de maintenance informatique de l'agence de presse francophone Guysen Israël, « *l'attaque était très sérieuse et aurait pu avoir des conséquences désastreuses si nous n'avions pas intercepté le virus à temp*s ». Figurent au palmarès impressionnant de ce viol virtuel les plus importants sites du pays comme les banques Hapoalim (la plus grande du pays) et Otsar Ha-Hayal, BMW Israël et l'hôpital Rambam de Haïfa, entre autres. Le groupe, qui dit être composé de six jeunes âgés de moins de 20 ans, selon Guysen, était déjà connu des services de police du web israélien.

« *Les crackers marocains sont les deuxièmes plus forts au monde après les Brésiliens* », selon Computer Coordination Center of Morocco (CCC).

1-7. Les hacktivistes

[29] Voir par exemple le Dahir de 1970 sur la propriété littéraire et artistique abrogé par le Dahir de 2000 sur les droits d'auteurs et droits voisins.

Le **hacktivisme** est une contraction de *hacker* et activisme. Ici se trouvent simultanément les savoir-faire technologiques et analyses politiques. Le "hacktiviste" infiltre des réseaux, toutes sortes de réseaux, et pas seulement les réseaux électroniques, mettant son talent au service de ses convictions politiques, et organisant des opérations *coup de poing* technologiques : piratages, détournements de serveurs, remplacement de pages d'accueil par des tracts[30].

Au Maroc, le hacktivisme est en train de prendre son ampleur : Depuis 2006 les hacktivistes marocains[31] en su faire parler d'eux et ont gagné de la notoriété en matière de cyber-activisme, selon Jeffrey Carr dans son livre Inside Cyber Warefare: Entre juin et novembre 2006 un groupe marocain intitulé « Team-evil » ont piraté plus de 8000 sites israéliens dont 171 sites gouvernementales et de grandes marques. Les pirates israéliens ont répondu à leur manière, le groupe « TEAM Good » ont piraté OMIHOST l'un des plus grands hébergeurs marocains à l'époque en défigurant les pages d'accueil de 250 sites internet marocains.

La même année a connu une vague de cyber-attaques contre le web danois, plus de 1000 sites danois ont été piraté pour protester contre la publication de caricatures offensives du prophète **Mohammed** selon zone-h.

[30] http://fr.wikipedia.org/wiki/Hacktivisme consulté le 2/6/2012

[31] Un arrière plan noir, le drapeau marocain et la musique du hymne national jouée en arrière plan », c'est à ça que ressemble les pages d'accueil de plusieurs sites piratés par des pirates marocains, les motivations des attaquants diffèrent et sont souvent accompagnées de revendications ou protestations contre un fait, les acteurs du déface sont parfois des particuliers qui défendent une cause, des rassemblements ou mouvements qui prétendent « défendre les intérêts suprêmes du Royaume

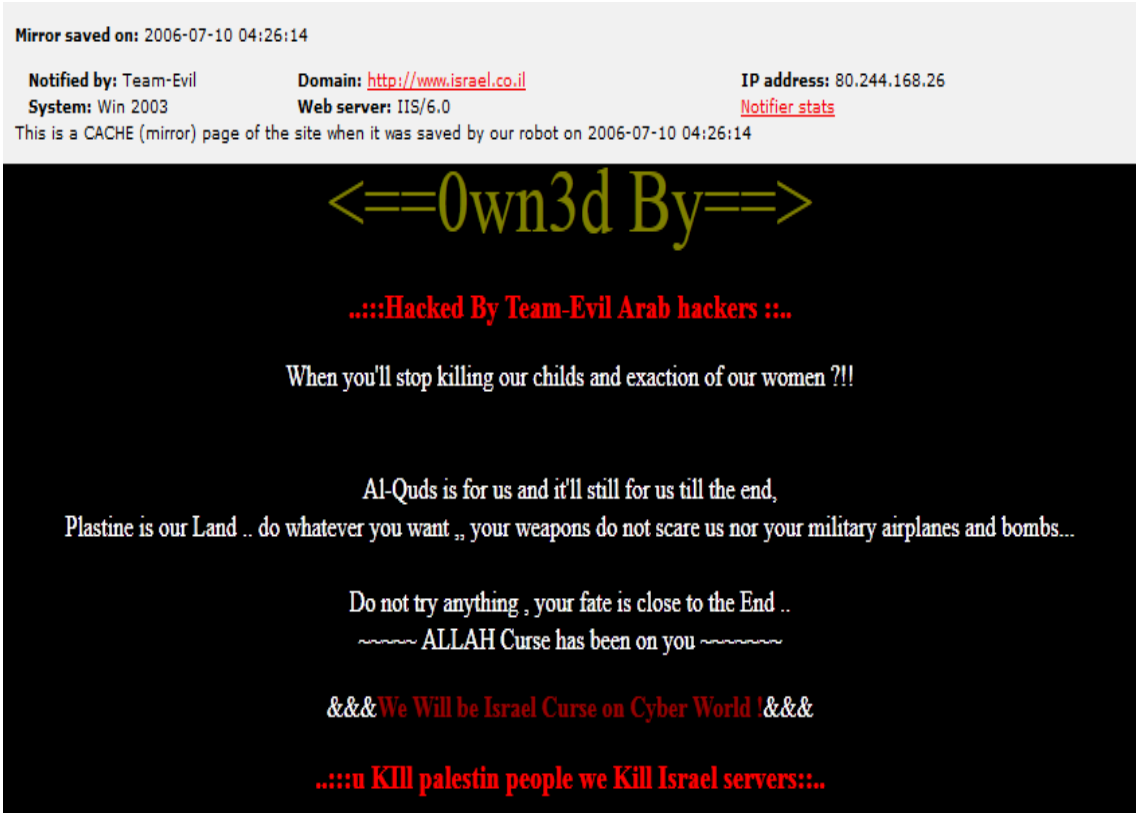

Figure 2 : *Image de page d'accueil du site* www.israel.co.il *après avoir être piraté par le groupe « Teamevil »*32

En Mai 2009, des hacktivistes marocains, attaquent une 50ène de sites algériens ainsi que plusieurs sites du Polisario dont polisario-confidential.org et le site officiel de Tindouf (tindouf.org)[33].

Le lundi 11 juin 2012 des hacktivistes marocains nommés « ***morrocan force of deterrence*** » On pu pirater le site web de l'ambassade de polisario en Algérie amb-rasd.org (voir figure 3 page suivante)

32 http://www.zone-h.org/mirror/id/4282699
33 http://www.mcherifi.org/hacking/cyber-activisme-au-maroc.html

Figure 3 : *Image de page d'accueil du site d'ambassade de polisario en Algérie amb-rasd.org après avoir être piraté par le groupe marocains « morrocan force of deterrence »*

2. Les différentes formes de la cybercriminalité

Sans être exhaustif, on peut aujourd'hui repérer les risque qui portent atteinte aux systèmes d'information et ceux qui utilisent ou exploitent un système d'information pour commettre un délit et créer toutes sortes de préjudice.

2-1. Typologies de risques cybercriminelles

Le tableau suivant dresse une typologie de ces risques liés à la cybercriminalité :

TYPES	MODALITES
Sabotage	Destruction physique, bombe logique, déni de service
Vol	Vol de support, clé USB, documents, portable, vol d'identité, copie illicite de données
Intrusion	Spoofing, Scaming, usurpation d'identité
Fraude	Spamming/phisching, escroquerie
Piratage	Contrefaçon de contenu numérique, de logiciel, de carte bancaire et de carte à puce

Atteinte à la vie privée	Logiciel espion, cookies, exploitation frauduleuse de données personnelles
Contenus illégaux	Pédopornographie via internet Délit de presse, diffamation, injures, menaces, etc.

Tableau 3 : *typologie des risques liés à la cybercriminalité*[34]

Concernant les entreprises, quatre grands types de menaces visent particulièrement les sociétés, à savoir les vols de supports et de données, les intrusions dans les réseaux, les interceptions de communications ou de flux de données et enfin la manipulation des employés et des concurrents par le biais notamment du « *social engineering* »[35].

2-2. Les multiples visages de la cybercriminalité

La cybercriminalité à multiples visages. Chaque jour, elle se manifeste d'une nouvelle manière. Tantôt elle n'est que la virtualisation d'anciennes méthodes d'escroqueries tantôt elle nous surprend par le caractère « novateurs » du monde opératoire qu'elle applique. c'est ce qui a été confirmé par Mr Bouchaîb RMAIL « *il ressort de l'analyse des différentes infractions en matière informatique ou liées aux nouvelles technologies de l'information et de la communication, que ces infractions qui constituent de sérieuses menaces attentatoires à la stabilité économique et à l'information en tant que nouvelle valeur économique ou autre, dans le contexte économique actuel, peuvent être répartit en deux catégories ; des menaces classiques et de menaces émergentes* »[36].

Dans notre étude, il nous a semblé pertinent d'appréhender les différentes formes de cybercriminalité à travers les objectifs visés par rapport aux quatre piliers de la sécurité à savoir : la disponibilité, l'intégrité, la

[34] Tableau élaboré d'après *le livre bleu des assises de la Sécurité et des Systèmes d'information*, octobre 2009. site : www.lesassisesdelasecurite.com
[35] QUEMENER. M, CHARPENEL. Y , op.cit. p9
[36] RMAIL. B, pp.cit. P 58

confidentialité et la preuve[37]. Et nous allons classer ces actes cybercriminels en deux catégories :

- Les actes cybercriminel dans lesquels l'ordinateur comme moyen ou cible.
- Les actes cybercriminels dans lesquels l'ordinateur est un facilitateur de l'infraction.

2-2-1. Les actes cybercriminel dans lesquels l'ordinateur comme moyen ou cible.

L'appréhension de cette catégorie sera faite comme suit :

- ✓ Les actes portant atteinte à la confidentialité : *phishing* et attaques virales
- ✓ Les actes portant atteinte à la disponibilité : le DoS et le DDoS
- ✓ Les actes portant atteinte à l'intégrité : le deffacement des sites WEB
- ✓ Les actes portant à la preuve.

A. Les actes portant atteinte à la confidentialité : phishing et attaques virales.

❖ Le phishing

Un nouveau type de pêche fait fureur sur le Web : le phishing contraction des mots anglais *fishnig*, qui veut dire pêche en français, et phreaking, désignant le pirate de lignes téléphonique. Pratiquée par les pirates, cette technique profite notamment de la naïveté des internautes pour leur soutirer leurs données personnelles (notamment bancaires) afin effectuer des achats avec leur numéro de carte bancaire.

Aujourd'hui, à l'ère du tout numérique, ce procédé représente le nec plus ultra de ce qu'il est possible de faire en ingénierie sociale. Même lorsqu'elles

[37] NB : nous tenons à préciser que plusieurs typologies d'attaques peuvent avoir un impact sur plusieurs piliers de sécurité ; à titre d'exemple, une attaque virale peut avoir comme conséquence une atteinte à la disponibilité, à l'intégrité, à la confidentialité ou à la preuve dépendamment de la nature des objectifs visés.

s'appuient sur des techniques basiques, ces attaques font de nombreuses victimes par la simple manipulation des esprits.

Les risques sont d'autant plus élevés que ce genre d'escroqueries ne concerne pas uniquement les banques. Il ya aussi les sites de commerce électronique et ceux des opérateurs télécom dans les lesquels on peut acheter des cartes prépayé ou des forfaits. Très souvent, plus la ficelle est grosse, plus l'attaque a de chance de réussir ! en 2005 ; il ya eu une tentative de *phishing* qui reprenait les logos de CIA et du FBI », déclare Yves Crespin de la BEFTI. Le texte de l'e-mail était à peu près celui-ci : « *vous avez surfé sur des sites interdits et vous avez été repérés par nos services (services concernés auxquels il est fait référence : la CIA et le FBI). Mettez vous rapidement en relation avec nous par retour d'e-mail, sous peine de poursuite. Indiquez nous toutes vos coordonnées y compris bancaires et codes secrets*…)[38].

Certaines études classent les techniques du *phishing* en deux catégories :

✓ *Les techniques artisanales :* tendent toutes à harponner la victime à travers le courrier électronique, les sites Web malveillants, la messagerie instantanée et les PC domestiques piratés. Les mécanismes d'attaques réalisés sont de deux ordres : l'attaque par le milieu et l'attaque par obfuscation de l'URL[39].

✓ Les techniques industrielles : elles sont de nombre de trois : le pharming, les botnets et le vishing.

- Le pharming : est une technique qui tend à piéger les navigant sur le net, non pas en s'attaquant à leurs propres ordinateurs, mais, en s'attaquant aux infrastructures du réseau Internet, en réalisant le

[38] Filiol.E., Richard.P, « Cybercriminalité enquête sur les mafias qui envahissent le Web », p 39. DUNOD, 2006

[39] L'attaque par obfuscation de l'URL est réalisée par l'utilisation des noms de domaines modifiés pour faire livrer à toute personne se connectant de fournir des informations confidentielles sur le site dont le nom de domaine est modifié et sous le contrôle de l'attaquant.

détournement de millions de connections vers le site sous le contrôle de phisher.

- Les botnets : il s'agit d'un réseau de machines zombies, communiquant entre elle à l'aide de logiciel malveillants, pour accéder à travers ces machines à des informations confidentielles susceptibles d'êtres exploitées à travers l'espionnage de claviers
- Le vishing : il s'agit de réaliser des attaques à l'aide l'utilisation de nouveau moyen de communication. Selon cette technique, l'attaquent met en place des serveurs de VOIP qui composent de manière aléatoires des numéros de téléphones. Lorsque les victimes décrochent, elles ont droit à un message enregistré sur une boite vocale les incitant à appeler un serveur vocal dont le numéro est fourni et décliner les identifiants de leurs cartes bancaires ou autres informations confidentielles par saisie sur le clavier du téléphone. Une variante de cette technique peut substituer de simples courriers électroniques ou des SMS au serveur vocal.

❖ Les attaques virales

L'époque des virus infectant des machines pour rendre indisponible un service donné et gêner le travail de l'utilisateur est révolue. Aujourd'hui, l'attaque virale est de plus en plus orientée vers l'appât de gain. Pour y parvenir, les infections dues à ces virus sont dirigées pour rechercher des données sensibles et les envoyer à l'adresse électronique d'un tiers sur ordre du concepteur du virus.

Les virus se sont des programmes informatiques malins, tendant à réaliser un résultat dommageable pour le propriétaire d'un ordinateur ou d'un réseau informatique. On distingue entre deux types de virus : virus informatiques et virus d'internet.

- ***Les virus informatiques***

Un virus est un programme capable de se reproduire dans un ordinateur, pouvant infecter d'autres programmes et, ainsi, se transmettre d'un ordinateur à l'autre, si l'on copie le programme infecté sur un ordinateur sain. S'ils ne faisaient que se reproduire, les virus n'inquièteraient personne. Malheureusement, ils peuvent être programmés pour être nuisibles, par exemple, en effaçant les données de la machine sur laquelle ils s'exécuteront à une date précise. Les virus informatiques peuvent être répartis en deux grandes catégories : les virus classiques et les virus d'internet[40].

- ***Le ver***

Un ver diffère de virus au sens qu'il se transfère de lui-même d'un ordinateur à l'autre au travers d'un réseau. L'exemple le plus connu et le plus dévastateur est sans doute d'ARPANET ; qui paralysa le réseau en 1988.

- ***Le cheval de Troie***

Appelé aussi malware, un cheval de Troie est un programme qui n'est pas ce qu'il à l'air d'être. Par exemple, vous recevrez par la poste une publicité, sous la forme d'une disquette contenant la version de démonstration d'un traitement de texte. Si, en plus de faire office de traitement de texte son programmeur a décidé de lui faire rechercher la liste de toutes les applications contenues dans votre ordinateur et d'effacer les fichiers des logiciels de traitement de texte concurrents, il s'agit d'un cheval de Troie.

Classement	Nom	%d'utilisateurs uniques attaqués*
1	DangerousObject.Multi.Generic	35,56%
2	Trojan.Win32.Generic	31,49%
3	Trojan.Win32.Starter.yy	13,92%
4	Virus.Win32.Sality.bh	12,61%

[40] On appellera « virus classique » les virus qui ont été développé en premier lieu ou en priorité avec des langages de programmation classique, pour être propagés soit, intentionnellement, soit à l'aide de moyen physique (disquette, CD Rom…) quant aux « virus d'internet » se sont les virus adaptés aux transformation de l'informatique par le biais de net autrement dit de nouveaux langages de programmation adaptés à la navigation sur Internet on été apprivoisés par les créateurs de virus, tel que Java ou ActivX

5	Net-Worm.Win32.Kido.ih	10,79%
6	Virus.Win32.Sality.aa	9,32%
7	Trojan.Win32.AutoRun.g en	8,71%
8	Net-Worm.Win32.Kido.ir	8,63%
9	Hoax.Win32.ArchSMS.gen	8,60%
10	HiddenObject.Multi.Generic	6,58%
11	AdWare.Win32.InstallCore.gen	6,41%
12	Virus.Win32.Generic	6,18%
13	Virus.Win32.Nimnul.a	5,83%
14	Worm.Win32.Generic	5,52%
15	Trojan.WinLNK.Runner.bl	4,56%
17	Trojan-Dropper.VBS.Agent.bp	3,61%
18	Virus.Win32.Sality.au	3,51%
19	Trojan.Script.Generic	3,38%

Ces statistiques sont les verdicts détectés par les modules OAS et ODS de l'Antivirus transmis par les utilisateurs de logiciels de Kaspersky Lab qui ont accepté de transmettre des statistiques. Pourcentage d'utilisateurs uniques sur les ordinateurs desquels l'Antivirus a détecté l'objet en question, par rapport à l'ensemble des utilisateurs uniques des produits de Kaspersky Lab chez qui l'Antivirus s'est déclenché.

Tableau 4 : *Top 20 des objets découverts sur les ordinateurs malveillants*[41]

B. Les actes portant atteinte à la disponibilité : le DoS et le DDoS

La disponibilité peut aussi être atteinte suite à des attaques physiques, ne requérant que peu de technologies, sur les installations informatiques ou le câblage des réseaux. Mais la forme d'attaque la plus dangereuse et la plus répandue dans l'univers Underground reste incontestablement l'attaque DDoS.

Le DoS et le DDoS : Définition

Les attaques en Déni de Service (DoS) ont pour objectif de consommer tout ou partie des ressources d'une cible, afin de l'empêcher de pouvoir rendre ses services de façon satisfaisante. En effet, les routeurs qui ont la charge de fluidifier et de rationnaliser le trafic IP ne peuvent quelques fois plus supporter une telle masse de requêtes. Les premiers types d'attaques en Dénis de Service

[41] http://www.viruslist.com/fr/analysis?pubid=200676286

ne mettaient en cause qu'un seul attaquant (DoS), mais rapidement, des attaques évoluées (DDoS) sont apparues, impliquant une multitude d'ordinateurs « zombies » (voir figure).

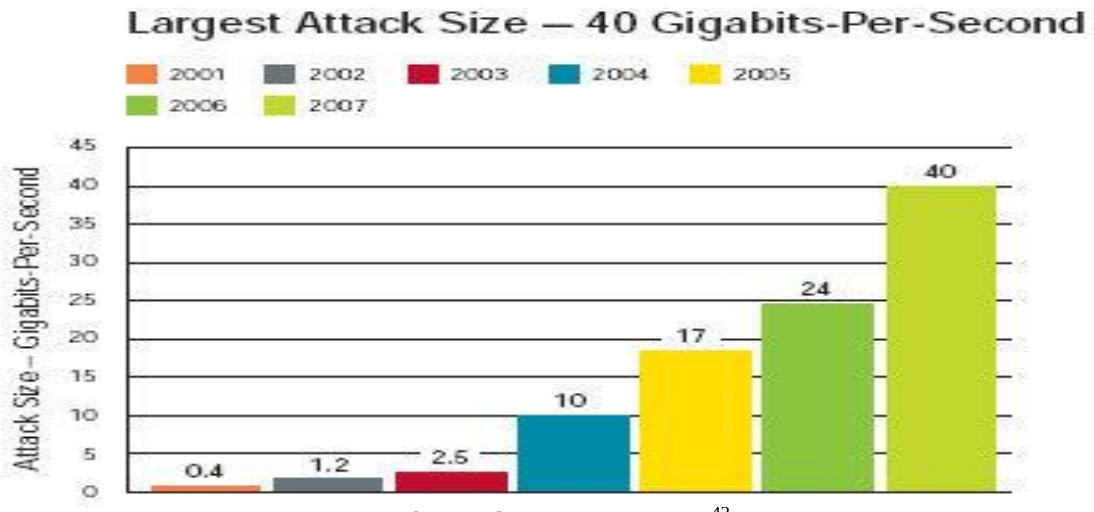

Figure 4 : *Evolution des attaques DDoS*[42]

C. Les actes portant atteinte à l'intégrité : le défacement des sites WEB

L'atteinte à l'intégrité est rarement l'objet d'attaque cybercriminelle ayant pour but l'appât de gain. Cependant, cependant comme cela a déjà était le cas, des organisations peuvent recourir aux services de cybercriminelle afin d'altérer des données d'une organisation cible. Il s'agit notamment d'attaques ayant pour objet de nuire à l'image de marque d'une entreprise concurrente ou d'une organisation « ennemie ». Le déffacement des sites web reste la meilleure manifestation de ce genre d'attaque. Il s'agit d'attaques provoquées par l'utilisation de failles présentes sur une page Web ou tout simplement une faille du système d'exploitation du serveur Web. La plupart du temps, les sites é le sont uniquement sur la page d'accueil.

Au Maroc l'ampleur du phénomène de déffacement des sites web est arrivée à un point tel que certaines analyses avancent que les sites marocains constituent un terrain d'entrainement pour des pirates étrangers[43].

[42] http://www.arbornetworks.com/report
[43] ELAZZOUZI. A, la cybercriminalité au Maroc ; op.cit ; P 58

Voici une liste non exhaustive des sites web institutionnels des organismes gouvernementaux ayant fait l'objet de défacement :

Tableau 5: *liste des sites web marocains défacés*[44]

Date	Attaquant	Domaine	Système
2009/05/28	Dr.Anach	www.marocainsdumonde.gov.ma/im...	Linux
2009/04/27	Hmei7	www.habous.gov.ma/sidishiker/i...	Win 2003
2009/01/08	GANG hackers ARABS	Docs.justice.gov.ma/ang.txt	Win 2003
2008/11/21	Old.Zone	www.equipementransport.gov.ma/...	Win 2003
2008/11/20	Old.Zone	www.mtpnet.gov.ma/index.htm	Win 2003
2008/09/23	ExSploiters	www.lagencedusud.gov.ma	Win 2003
2008/09/16	NetKiller	www.affaires-generales.gov.ma/...	Win 2000
2008/08/17	mor0ccan nightmares	agadir-indh.gov.ma	Linux
2008/08/17	mor0ccan nightmares	www.essaouira-indh.gov.ma	Linux
2008/08/04	Sm4rT Security Cr3w	www.dapr.gov.ma	Linux
2008/08/02	Handrix	www.invest.gov.ma/all4one.htm	Win 2003
2005/01/18	Fatal Error	www.mhu.gov.ma	Win 2000

D. Les actes portant à la preuve

Inéluctablement les cybercriminels ne cessent plus de développer leurs techniques pour commettre leurs infractions. Ils visent même la preuve en tant que pilier de sécurité. Qui dit preuve dit traçabilité, c'est-à-dire lors d'une attaque, l'information contenue dans les fichiers logs peut être vérifiée pour détenir les traces de l'attaque et aboutir à une preuve accusatrice. Or cette preuve pourra être détruite par un cybercriminel qualifié qui a intérêt à effacer les fichiers logs ou à modifier leur contenu ;

[44] Idem

2-2-2. Les actes cybercriminels dans lesquels l'ordinateur est un facilitateur de l'infraction

Plusieurs menaces classiques ont trouvé dans l'ordinateur le moyen adéquat qui facilite leur commission, et qui leur donne l'aspect d'acte cybercriminel puisqu'ils sont commises dans le cyberespace. Il s'agit notamment de l'espionnage et activité de renseignement, blanchiment de capitaux, fraude à la carte bancaire, le cyberterrorisme…

A. Espionnage et activité de renseignement

Cet espionnage se déploie notamment dans le domaine économique et a donné naissance à un nouveau concept « l'infoguerre »[45]. Il vient ainsi à recouvrir les pratiques de ciblage des informations et des fonctions informationnelles d'un concurrent de la part d'une entreprise, qui tout en cherchant à protéger son propre système, aspire à acquérir des informations pour servir ses objectifs tactiques et stratégiques.

Les cibles de l'infoguerre peuvent être aussi l'Etat et les individus : l'Etat peut être attaqué dans son propre système d'information et les individus se voient menacés notamment par l'introduction frauduleuse dans les bases de données : vols d'identités…

B. Blanchiment de capitaux[46]

Le blanchiment d'argent est le processus consistant à dissimuler la source de l'argent ou des biens tirés d'activités cybercriminelles. Une grande variété d'activités illégales est motivée par le profit, notamment le trafic des stupéfiants, la contrebande, la fraude, l'extorsion de fonds…

Sur internet, en raison notamment de la multiplication des banques en ligne, des casinos virtuels, des sites de paris en ligne et des possibilités de

45 Né dans un contexte militaire au moment de la guerre du Golfe, le concept d'infoguerre (traduction de l'américain Infowar, contraction de Information Warfare)

46 Sanctionné par la loi 43-05 relative à la lutte contre le blanchiment de capitaux promulguée par le Dahir n° 1-07-79 du 11 avril 2007

placement en ligne, les possibilités de blanchiment d'argent sont illimités[47]. Les intermédiaires recrutés sont qualifiés de « mules ».

C. Fraude à la carte bancaire

Avec Internet, la fraude est devenue plus facile, car la puce de la carte bancaire n'intervient pas. Il suffit souvent d'avoir les quelques numéros inscrits sur le support. Les fraudeurs disposent de différents moyens. Le numéro peut être créé par *"moulinage"* (à l'aide de générateurs aléatoires). Il peut aussi être relevé à l'insu du porteur de la carte : avec des logiciels espions sur l'ordinateur du consommateur, ou par la méthode du *"phishing"* (hameçonnage), où le consommateur entre ses données personnelles sur un site, croyant qu'il s'agit d'un tiers de confiance

Le Maroc n'échappe pas au phénomène de fraude à la carte bancaire. En effet, le nombre de cartes bancaires contrefaites au Maroc est passé de 1.694 cartes en 2000 à plus de 6000 en 2008.

D. Pédophilie sur internet

Les réseaux pédophiles continuent toujours à faire de l'internet une véritable zone de non-droit. En effet, grâce à la diffusion des technologies assurant l'anonymat, notamment le chiffrement des courriels et l'utilisation de proxy, il est devenu extrêmement difficile de surveiller les activités des réseaux pédophiles.

Selon un chiffre désormais largement diffusé, un mineur sur cinq a été confronté à des avances sexuelles sur internet.

Au Maroc plusieurs affaires de pédophilies ont été marquées par exemple :

En 2005 : un journaliste belge de l'hebdomadaire « le Soir » prenait des photos pornographiques des jeunes filles d'Agadir et les publiait sur un site pornographique. Parmi ses victimes, il y avait des prises montrant de filles mineures.

47 ELAZZOUZI. A , op. cit, P 72

Conclusion du premier chapitre

La cybercriminalité est un business organisé, facile, à faible risque et surtout très rentable. De nombreux utilisateurs peu scrupuleux et en quête d'argent facile n'hésitent pas à s'y lancer. L'incompréhension qui entoure l'univers de la sécurité de l'information leur facilite grandement la tâche. L'être humain reste le maillon faible de la chaîne de la sécurité et il faut le considérer en tant que tel.

La multiplication des actes cybercriminels cause d'un coté des préjudices aux organisations qu'au pays, et d'un autre elle rend les internautes moins confiant en ligne. Donc les états doivent riposter cette menace. Le Maroc appartenant à ce village planétaire doit réagir face à ce danger, c'est ce qu'on va détailler dans le chapitre suivant.

Chapitre 2 : les efforts du Maroc pour lutter contre la cybercriminalité et instaurer la confiance numérique

Certes, l'internet a transformé le monde en village planétaire, la démocratisation de l'accès à l'informatique et la globalisation des réseaux ajoutés à l'anonymat que procure l'internet ainsi que l'adoption à grande échelle du Web 2.0 ont fortement favorisé le développement de la cybercriminalité partout dans le monde. Le Maroc fait partie de ce village, régi par les moyens de télécommunication les plus sophistiqués permettant de négocier, de dialoguer et d'échanger en temps réel. Nous sommes alors exposés aux conséquences de la cybercriminalité au même titre que nos partenaires européens par exemple. Le nombre d'internautes marocains, qui n'a pas cessé de croître ces dernières années, continue de grimper d'une façon exponentielle. Cette croissance, tirée notamment par le haut débit et l'Internet 3G, couplée à l'anonymat et au faible risque de se faire arrêter, joue un rôle favorable pour le développement de la cybercriminalité. En outre, l'absence d'une véritable mise à niveau de l'arsenal juridique et l'inexistence d'institutions chargées des investigations, de la veille et de la répression risquent de faire du Maroc un véritable paradis pour les cybercriminels. Chose qui provoquera une certaine méfiance envers les opportunités offertes par l'internet (achat en ligne, e-Commerce, paiement par carte bancaire…)

Face à cette menace grandissante qui devient plus visible pour les masses, le Maroc essaie de redoubler ses efforts pour combattre la cybercriminalité et instaurer un climat de confiance numérique. En effet de nouvelle lois on été promulguées, de nouvelles organisations ont été créées et un programme ambitieux de confiance numérique proposé dans le cadre de la stratégie « Maroc Numérique 2013 » a été lancé. Ainsi, la culture de sécurité, bien qu'elle

ne soit que dans un état embryonnaire, commence à s'installer non seulement dans les institutions publiques et privés mais aussi dans l'esprit de tout chacun.

Dans ce cadre le présent chapitre, va mettre en exergue au début les enjeux de lutte contre la cybercriminalité (section1), après nous mettrons l'accent sur la cybercriminalité de portée marocaine ainsi que les ripostes juridiques (section 2), et enfin nous parlerons du défi de confiance numérique (section 3).

Section 1 : Les Enjeux de lutte contre la cybercriminalité

Pour accélérer les enquêtes et automatiser les procédures de recherche, les agences de répression peuvent aujourd'hui exploiter la puissance, toujours plus grande, des systèmes informatiques et profiter des logiciels sophistiqués utilisés en criminalistique.

Les enjeux en matière de lutte contre la cybercriminalité sont particulièrement forts aujourd'hui car il s'agit d'une part de lutter contre ce phénomène tout en préservant les libertés des individus ainsi que leur sécurité.

Avant d'étudier ces deux éléments que nous allons les considérer comme *enjeux spéciaux* de lutte contre la cybercriminalité (2), il est dans l'opportun d'examiner quelques *enjeux généraux* de lutte contre cette délinquance (1).

1. Enjeux généraux

Les enjeux généraux de lutte contre la cybercriminalité représentent la réponse à la question : quel danger suscite cette lutte urgente ?

La cybercriminalité et ses méthodes s'évoluent jour après jour en tirant profit de la dépendance mondiale à l'égard des TIC, de nombre croissant des internautes, de la vitesse de processus d'échange des données, et surtout de l'insuffisance de mécanisme de contrôle.

L'intervention étatique et celle des criminalistiques doivent intervenir notamment dans les niveaux suscités.

1-1. Dépendance à l'égard des TIC

De nombreuses communications de la vie quotidienne s'appuient aujourd'hui sur les TIC et les services Internet. Ainsi les appels vocaux sur IP et les communications par courriel. Les bâtiments, les voitures et les services aériens reposent également sur les TIC pour effectuer des fonctions de commande et de gestion, de même que l'approvisionnement en énergie et en eau ainsi que les services de communication. Et il y a toutes les chances pour que ces nouvelles technologies continuent de s'installer dans notre vie quotidienne.

Cette dépendance croissante à l'égard des TIC augmente la vulnérabilité des systèmes et des services liés aux infrastructures essentielles. Des interruptions de service, même de courte durée, peuvent entraîner de lourdes pertes financières. Les services civils (entreprises de commerce électronique, etc.) ne sont pas les seuls concernés, la dépendance à l'égard des TIC met aussi gravement en danger les communications militaires. Les infrastructures techniques existantes présentent plusieurs faiblesses, parmi lesquelles la monoculture ou homogénéité des systèmes d'exploitation. Bien des particuliers et des PME utilisent en effet le système d'exploitation de Microsoft, cible dès lors privilégiée des cyberdélinquants.

La dépendance de la société vis-à-vis des TIC n'est pas un phénomène propre aux pays occidentaux : les pays en développement aussi sont confrontés aux problèmes de prévention des attaques visant leurs infrastructures et leurs utilisateurs. Grâce au développement de technologies moins onéreuses en termes d'infrastructures, telles que WiMax[48], les pays en développement peuvent aujourd'hui proposer des services Internet à un plus grand nombre d'utilisateurs. En théorie, ces pays devraient éviter les erreurs de certains pays occidentaux, qui

[48] WiMAX (Worldwide Interoperability for Microwave Access) Egalement connu sous la désignation d'IEEE 802.16, le Wimax est un standard de transmission sans fil à haut débit. Fonctionnant à 70 Mbit/s, il est prévu pour connecter les points d'accès Wi-Fi à un réseau de fibres optiques, ou pour relayer une connexion partagée à haut-débit vers de multiples utilisateurs. Avec une portée théorique de 50 km, il devrait permettre, à terme, le développement de réseaux métropolitains (MAN) reposant sur un unique point d'accès, au contraire d'une architecture basée sur de nombreux points d'accès Wi-Fi.

ont axé leur développement sur la maximisation de l'accessibilité sans investir notablement dans la protection. Selon certains experts américains, les attaques contre le site officiel des organisations gouvernementales d'Estonie n'ont pu porter leurs fruits qu'en raison de l'insuffisance des mesures de protection. Or les pays en développement ont une occasion exceptionnelle d'intégrer des mesures de sécurité dès les premières phases de mise en œuvre. Cela suppose certes des investissements initiaux plus importants, mais l'intégration de mesures de sécurité à un stade ultérieur pourrait se révéler plus coûteuse sur le long terme.

Il importe donc de développer des stratégies de prévention et de concevoir des contre-mesures, notamment de mettre au point et de promouvoir des moyens techniques de protection, mais aussi une législation adaptée et suffisante, qui permette aux services de répression de lutter efficacement contre la cybercriminalité.

1-2. Nombre d'utilisateurs

La popularité d'Internet et de ses services augmente rapidement et on compte aujourd'hui un milliard d'internautes dans le monde. Au Maroc, le Marché de l'Internet a poursuivi sa forte progression au cours de l'année 2010, avec une croissance annuelle du parc d'abonnés de 57,3% (1,86 millions à fin 2010, contre 1,18 à fin 2009). Le taux de pénétration au sein de la population a suivi une courbe parallèle, avec un taux de 5,9% à fin 2010 (contre 3,8% une année auparavant)[49].

Il est difficile d'estimer combien de personnes utilisent Internet dans le but de mener des activités illicites, mais, quand bien même ils ne représenteraient que 0,1% des internautes, les cyberdélinquants dépasseraient un million. Bien que les taux d'utilisation d'Internet y soient inférieurs, il n'est pas plus facile de promouvoir la cybersécurité dans les pays en développement, car les cyberdélinquants peuvent agir de n'importe quel point du globe.

[49] Rapport Annuel de l'ANRT, année 2010 disponible sur le site :
http://www.anrt.ma/sites/default/files/rapportannuel/Rapport%20annuel%202010%20_fr.pdf

Etant donné qu'il est relativement difficile d'automatiser les processus d'enquête, l'augmentation du nombre d'internautes est source de difficultés supplémentaires pour les services de répression. S'il est relativement facile d'effectuer une recherche de contenus illicites à partir de mots-clés, la recherche d'images est plus problématique. Les approches fondées sur la valeur de hachage par exemple ne portent leurs fruits que si l'image à analyser a préalablement été évaluée, la valeur de hachage stockée dans une base de données et l'image non modifiée.

1-3. vitesse de processus d'échange des données

Le transfert d'un courriel entre deux pays ne prend que quelques secondes. Si Internet a permis d'éliminer le temps de transport des messages – et c'est assurément l'une des raisons de son succès, les agences de répression disposent désormais de très peu de temps pour mener leurs enquêtes ou collecter des données, temps insuffisamment long pour des enquêtes classiques. On peut citer, à cet égard, l'échange de contenu pornographique mettant en scène des enfants. Les vidéos pornographiques étaient autrefois apportées ou livrées aux acheteurs, ce qui donnait aux services de répression l'occasion d'enquêter. Dans ce domaine, ce qui fait la différence entre l'avant et l'après Internet, c'est justement le transport: sur Internet, les films peuvent être échangés en quelques secondes[50].

L'exemple du courriel met également en évidence l'intérêt de disposer d'outils ultrarapides permettant d'intervenir immédiatement. En effet, pour remonter jusqu'aux suspects et les identifier, les enquêteurs ont souvent besoin d'accéder à des données qui sont effacées peu de temps après le transfert. Il est donc essentiel qu'ils puissent réagir très rapidement. Il paraît difficile de lutter efficacement contre la cybercriminalité sans une législation et des instruments adéquats permettant aux enquêteurs d'agir immédiatement et d'empêcher que des données ne soient effacées.

[50] GERCKE. M, Comprendre la cybercriminalité: Guide pour les pays en développement, 2009. Op.cit

1-4. Insuffisance des mécanismes de contrôle

Tous les réseaux de communication de masse – des réseaux téléphoniques pour la communication vocale aux réseaux Internet – nécessitent une gestion centrale et des normes techniques qui garantissent une bonne opérabilité. Les études en cours concernant la gouvernance d'Internet tendent à indiquer que ce réseau n'est pas différent des autres infrastructures de communication nationales, voire transnationales : Internet aussi doit être régi par des lois. Les législateurs et les agences de répression ont d'ailleurs commencé à élaborer des normes juridiques, qu'il conviendra, dans une certaine mesure, de contrôler à un niveau central. A l'origine, Internet a été conçu comme un réseau militaire, reposant sur une architecture décentralisée afin de préserver la fonctionnalité principale intacte et opérationnelle, même en cas d'attaque de certains éléments du réseau. De par son infrastructure, Internet résiste donc aux tentatives externes de prise de contrôle. Il n'était pas prévu, dans le cahier des charges initial, de faciliter les enquêtes pour infraction ni de prévenir les attaques provenant de l'intérieur du réseau. Internet est aujourd'hui de plus en plus utilisé dans le civil. Cette évolution du secteur militaire vers le secteur civil s'accompagne d'une évolution de la demande en termes d'instruments de contrôle. Le réseau reposant sur des protocoles conçus à des fins militaires, il n'existe pas de tels instruments à un niveau central et il est difficile de les mettre en place a posteriori sans repenser profondément la conception globale. L'absence de ces instruments complique considérablement les enquêtes sur les cyberdélits[51].

De ce fait, les internautes peuvent, par exemple, contourner les techniques de filtrage en utilisant des services chiffrés de communication anonyme. Il est normalement impossible de se connecter aux sites Internet proposant des

[51] Idem

contenus illicites (pédopornographie par exemple) si les FAI en ont bloqué l'accès. Pourtant, en passant par un serveur de communication anonyme qui chiffre les transferts entre les internautes et le serveur central, il est possible de passer outre le blocage des contenus. En effet, les requêtes étant envoyées sous forme chiffrée, les FAI ne sont pas en mesure de les lire ni, par conséquent, de les bloquer.

2. Enjeux spéciaux de lutte contre la Cybercriminalité

Les enjeux en matière de lutte contre la cybercriminalité sont particulièrement forts aujourd'hui car il s'agit d'une part de lutter contre ce phénomène tout en préservant les libertés des individus ainsi que leur sécurité.

2-1. Protection des libertés individuelles

Si internet est un instrument de communication, il peut aussi menacer la vie privée des personnes, le développement des sites de socialisation donne une nouvelle dimension à ce risque, en encourageant les utilisateurs à sacrifier eux-mêmes leur propre intimité. En effet, le principe est d'inciter les internautes à révéler le maximum d'éléments de leur intimité, de préférence au plus grande de personnes.

Nous allons donc exposer la nature de ce risque surtout au niveau des réseaux sociaux, et par la suite nous proposerons quelques réponses.

2-1-1. Risques et réseaux sociaux

Les réseaux sociaux sont des plateformes de communication en ligne permettant de partager des intérêts communs. Ils connaissent aujourd'hui un succès extraordinaire, surtout auprès des jeunes entre 14 et 35 ans et si les raisons de cet intérêt croissant sont nombreuses les risques le sont aussi face à la protection des libertés individuelles.

Même si aucune loi n'interdit de divulguer sa propre vie privée, il n'en demeure pas moins qu'une telle révélation est forcément risquée dans la mesure où nul n'en connaît réellement les limites, ni dans l'espace ni dans le temps.

Tout d'abord, il est certain qu'offrir à une personne la possibilité de communiquer à l'ensemble de son entourage (familial, personnel, professionnel, etc.) des photographies et des informations sur un tiers crée un canal idéal pour relayer des atteintes à la vie privé et au droit à l'image, voire des diffamations. Tel est notamment le cas de la fonctionnalité qui permet de publier des photographies des ses amis sur sa fiche[52].

2-1-2. Réponses

Face à ce phénomène, il semble avant tout nécessaire de sensibiliser les jeunes utilisateurs à l'importance de la protection de leur vie privée, un moyen d'action pédagogique tant dans les établissements d'enseignement que sur Internet.

A coté de cette approche pédagogique, la réponse juridique ne doit pas être négligée ; or, force est de constater qu'à l'heure actuelle le droit n'apparaît pas toujours adapté aux risques particuliers que présentent ces sites. Il est ainsi inquiétant de constater que la plupart d'entre eux s'ouvrent aux annonceurs et dégagent leur responsabilité quant à l'utilisation qui peut être faite des informations échangées.

De surcroit, la complexité et l'absence fréquente de traduction française des conditions d'utilisation et des rubriques « *privacy* » permettent pas aux internautes -surtout au plus jeunes- de mesurer les conséquences de l'utilisation et de la communication de données personnelles sur ces sites.

Enfin, concernant les éventuels dommages qui peuvent être provoqués aux personnes par ces sites, les actions judicaires individuelles apparaissent à l'heure actuelle encore difficiles à mettre en œuvre. Déjà, de part l'incertitude du statu juridique des sites communautaires, entre éditeurs et hébergeurs, il est délicat de savoir quel régime leur appliquer et quelle procédure intenter en cas de contentieux.

[52] QUEMENER.M, CHARPENEL.Y, « CYBERCRIMINALITE droit pénal appliqué», op.cit p16. Ed ECONOMICA 2010.

Dans la mesure que où le nombre de victimes de telles atteintes sur ces sites s'accroit et que les conséquences pour elles peuvent être réellement graves, il semblerait nécessaire de leur proposer des procédures simples et rapides, adaptées à leur situation.

2-2. Sécurité

La sécurité des infrastructures d'information est devenue une préoccupation majeure des acteurs publics et privés qui mettent en place des parades technologiques et prennent des mesures pour lutter contre les contenus illicites ou préjudiciables sur Internet, de protéger les droits de propriété intellectuelle et les données à caractère personnel, et renforcer la sécurité des transactions électronique.

L'ouverture des entreprises sur le monde, grâce à Internet, et l'utilisation des réseaux d'information, les rendent plus vulnérables à des attaques informatiques venues de l'extérieur. La mise en place de mesures de sécurité constitue à cet égard une nécessité pour éviter les intrusions et pour protéger des documents confidentiels, des secrets de fabrique, ou encore les fichiers de l'entreprise. L'information traitée par les ordinateurs est désormais une ressource stratégique immatérielle qui nécessite une protection. Or, ces mesures de sécurité auront précisément pour objet de conserver trace des flux d'informations, directement ou indirectement nominatives, afin de mieux prévenir les risques et de repérer l'origine des problèmes.

La sécurité des systèmes d'information apparaît aujourd'hui comme l'une des réponses essentielles face à l'extension de la Cybercriminalité mais elle ne doit pas pour autant dériver vers une certaine censure sur « la Toile ». L'équipement croissant des ménages en ordinateurs et des connections à haut débit, accompagné d'une numérisation grandissante des échanges ont fini par sortir du champ des seuls spécialistes la question de cybersécurité[53].

[53] Idem

Section 2 : La cybercriminalité au Maroc et les ripostes juridiques

Au Maroc, on pourra sentir la gravité du phénomène à partir des chiffres alarmants des cas des délits informatiques enregistrés au niveau national (1) ; sachant bien qu'un grand nombre de crime de cyberespace ne sont ni déclarés, ni recensés pas les criminalistiques. Un autre problème majeur se pose c'est que l'Univers Underground marocain a plusieurs années d'avance par rapport à l'univers répressif (plusieurs actes cybercriminels tel l'escroquerie sont encore régit par le droit commun…). Il apparait donc utile de savoir la réponse de législateur marocain (2).

1. Illustration des cas cybercriminels au Royaume

1-1. L'affaire célèbre de Farid ESSABBAR

Août 2005 : les serveurs de Microsoft, CNN, ABC, du New York Times et de plus d'une centaine d'entreprises américaines sont attaquées par le virus ZOTOP, provoquant des dégâts évalués à plusieurs dizaines de millions de Dollars.

L'accusé Farid ESSABAR a été condamné pour "association de malfaiteurs, vol qualifié, usage de cartes bancaires falsifiées et accès illégal à des systèmes informatiques".

L'arrestation a eu lieu suite à une demande d'assistance émanant du FBI qui a retracé l'itinéraire du virus comme étant originaire d'un site informatique installé au Maroc. Les chaînes de télévision CNN et ABC News, le journal New York Times, l'aéroport de San Francisco, figurent parmi les victimes du virus "Zotob", qui s'est attaqué à plusieurs systèmes d'exploitation Windows 2000 de Microsoft.

Condamné à une peine de deux ans de prison ferme en première instance, puis à un an de prison ferme à la Cour d'appel de rabat, ESSABAR, âgé de 19 ans, va quitter sa cellule de la prison civile de Salé après y avoir passé 15 mois.

1-2. Piratage des sites gouvernementaux nationaux

- ✓ **docs.justice.gov.ma Portail documentaire du ministère de la justice piraté**

Le Portail documentaire du ministère de la justice a été piraté Le dimanche 28 mars 2010 par « !TeAm RaBaT-SaLe! »[54] (Voir figure 6)

Figure 5: *Image de page d'accueil du site docs.justice.gov.ma après avoir être piratée*[55]

Le dernier piratage répertorié de ce site date de décembre 2008, plus d'un an âpres ce hack les traces des fichiers crées par les premiers pirates sont encore accessibles sur le serveur a travers ce lien : hxxp://docs.justice.gov.ma/ang.txt

- ✓ **men.gov.ma ministère de l'éducation nationale et de l'enseignement encore piraté :** Après avoir été piraté en 2009 et 2010, une fois encore le site du Ministère de l'éducation nationale de l'enseignement supérieur de la

[54] http://www.hamza.ma/defacage/docs-justice-gov-ma-portail-documentaire-du-ministere-de-la-justice-pirate/ consulté le 10/6/2012
[55] Idem

formation des cadres et de la recherche scientifique[56] a été défacé le 4 mai 2011 par « Team Triple-Hack & Cr3zy H4Ck3r »[57].

- ✓ **plus de 3000 sites web marocains sous le contrôle de pirate :** Ces 3000 sites ne représentent qu'une infime partie des sites et serveurs qui sont contrôlés par les pirates.

DATE	NOTIFER	DOMAINE	OS
2012/03/15	mS_Dz	www.humanorrecrut.ma/afficher_...	Linux

Tableau 6 : *Liste non exhaustive des sites web marocain piratés par le groupe« hard hakerz*[58]

56 C'est le deuxième site gouvernemental marocain qui se fait piraté en 2011 après celui du ministère de la modernisation des secteurs publics en plus de 250 sites marocains dans le premier trimestre 2011 soit une augmentation de 300 % par rapport au premier trimestre 2010

57 http://www.hamza.ma/defacage/men-gov-maministere-de-l-education-nationale-de-l-enseignement-marocain-encore-pirate/ consulté le 10/6/2012

58 http://www.zone-h.org/archive/ip=196.217.246.65 consulté le 10/6/2012

2012/02/29	mS_Dz	www.lamalif.ma/fr/fer-forge-ar...	Linux
2011/11/30	nO lOv3	www.balmscruz.ma/fr/home.php	Linux
2011/11/15	kader11000	www.alpha.gov.ma	Linux
2011/10/14	islamic ghosts team	www.elg.ma/evenements.php	Linux
2010/04/25	hard_hakerz	www.belleauto.ma/sec.html	Linux
2010/04/25	hard_hakerz	www.belloul.ma/sec.html	Linux
2010/04/25	hard_hakerz	www.beltransfo.ma/sec.html	Linux
2010/04/25	hard_hakerz	www.belutrecht.ma/sec.html	Linux
2010/04/25	hard_hakerz	www.benahmed.ma/sec.html	Linux
2010/04/25	hard_hakerz	www.benbraline.ma/sec.html	Linux
2010/04/25	hard_hakerz	www.bendahoutrading.ma/sec.html	Linux
2010/04/25	hard_hakerz	www.benhidataoufik.ma/sec.html	Linux
2010/04/25	hard_hakerz	www.benhsaincom.ma/sec.html	Linux
2010/04/25	hard_hakerz	www.beni-house.ma/sec.html	Linux
2010/04/25	hard_hakerz	www.benmoussapromoteurimmobili...	Linux
2010/04/25	hard_hakerz	www.bennaji.ma/sec.html	Linux
2010/04/25	hard_hakerz	www.bennasserlab.com/sec.html	Linux
2010/04/25	hard_hakerz	www.benouanasetcie.com/sec.html	Linux
2010/04/25	hard_hakerz	www.bensinane.com/sec.html	Linux
2010/04/25	hard_hakerz	www.benson-shoes.ma/sec.html	Linux
2010/04/25	hard_hakerz	www.benyahya11.ma/sec.html	Linux
2010/04/25	hard_hakerz	www.benzitsud.com/sec.html	Linux
2010/04/25	hard_hakerz	www.benzrec.ma/sec.html	Linux
2010/04/25	hard_hakerz	www.berberepalace.ma/sec.html	Linux

1-3. Cartes bancaires marocaines piratées

Au Maroc de nombreux carders ont été arrêtés pour piratage des cartes bancaires. En 2005 Trois jeunes Rbatis dont deux adolescents de 17 ans ont été tout récemment interpellés par le service de la police du crime économique et financier. Suite à un avis d'Interpol du 12 avril dernier, les services policiers ont mis la main sur les trois hackers. Ils sont poursuivis pour « formation d'une bande criminelle afin d'escroquer des banques américaines et usurpation d'identité à travers Internet ». Ils travaillaient au sein d'un réseau international dont les autres membres sont encore en liberté. Les trois adolescents font partie d'un groupe de « carders » disséminés dans plusieurs pays. Dans le cas de nos « carders », on a retrouvé une liste de 600 clients américains qui disposent de comptes à la « Citizen's Bank ». Les « ***carders*** » marocains ont réussi à se procurer les informations confidentielles de leurs victimes, y compris le code

secret de leurs comptes. Ils y sont parvenus en construisant, l'été 2004, un faux portail de ladite banque et en invitant les clients à leur remettre ces informations. Ils ont fait de même avec les clients de *PayPal* et d'*Ebay*[59].

En 2008 : deux employés d'un centre d'appel basé à Casablanca, ont été interpellés par les agents de la brigade centrale de police. Ils ont détourné d'importantes sommes d'argent en utilisant les données de porteur de cartes (nom de titulaire de carte, PAN[60], date d'expiration, etc.) qu'ils enregistrent lors des conversations téléphoniques avec les clients français et transmettaient par la suite à une complice basée en France qui se charger d'acheter des biens sur Internet et de les revendre après.

En 2009 : un réseau international spécialisé dans la falsification de cartes bancaire a été démantelé par la police de Casablanca[61].

1-4. Cas de Cyberterrorisme au Maroc

En 2010 : Une cellule de cyberterrorisme préparant des attentats au Maroc et à l'étranger, a été récemment démantelée. Ce réseau, composé de six marocains, projetait des attentats contre plusieurs intérêts étrangers et des postes de sécurité dans le Royaume. Le réseau comptait également s'attaquer à différents foyers de tension dans le monde.

Avril 2012 : la Brigade nationale de la police judiciaire a démantelé une cellule terroriste constituée de trois personnes à Meknès. En plus des actes criminels visant la destruction et la mise en feu de locaux administratifs, les membres de cette cellule étaient actifs sur Internet, précise le ministère de l'Intérieur[62]

Les multiples cas de cybercriminalité suscités ci-dessus ne reflètent qu'une petite partie du phénomène. Chose qui confirme l'ampleur de cette

[59] http://www.bladi.net/des-marocains-impliques-dans-le-piratage-de-cartes-bancaires.html consulté le 1/6/2012
[60] Primary Account Number (PAN) est le numéro qui est composé des 16 chiffres qui figure sur la carte bancaire.
[61] ELAZZOUZI.A., op.cit, P71
[62] BENNANI. A, journal le soir article disponible sous l'adresse http://www.lesoir-echos.com/une-cellule-terroriste-demantelee-a-meknes/presse-maroc/49434/

menace. Face aux problèmes posés par ces nouvelles formes de délinquance, il est utile de s'interroger sur la capacité de dispositions, élaborées à une époque où l'informatique n'existe pas, d'appréhender les fraudes opérées par cette technique. Autrement dit, est ce que la législation marocaine représente-elle une riposte aux actes cybercriminelle ? Sachant bien que de nouvelles lois ont été promulguées pour le même but. La réponse à cette question fera l'objet de la sous section suivante.

2. La législation marocaine et l'acte cybercriminel

Auparavant, au Maroc, la position de la doctrine a varié entre l'interprétation des règles classiques du code pénal et l'appel à la promulgation de nouvelles règles spécifiques.

En effet, quelque soient les solutions juridiques envisagées, toute solution reste inopérante sans l'intervention de législateur. Ainsi la cour d'Appel de Casablanca, à l'opposé du Tribunal de première instance, n'a pas pu, dans les années 80, condamner des personnes poursuivies pour avoir, successivement, effectué des manipulations téléphoniques et utilisé abusivement la carte de paiement, en l'absence des textes législatifs en matière informatique[63].

En fin de compte, la spécificité du nouveau phénomène technologique, a mis en relief les limites des dispositions pénales classiques. En plus de ces facteurs sociologiques et juridiques, d'autres facteurs, notamment des facteurs économiques et sécuritaires[64], ont accéléré l'intervention du législateur marocain[65].

Les textes sanctionnant la cybercriminalité peuvent être répartis en deux catégories : des règles d'ordre générales et des règles d'ordre particulier.

2-1. Règles d'ordre général

[63] Les arrêts de la cour d'appel de Casablanca du 2 décembre 1985 et du 24 avril 1990
[64] En l'occurrence la mondialisation et le terrorisme
[65] GHALI. A, de la criminalité informatique au Maroc, Revue Marocaine de Droit des Affaires et des Entreprises n° 17-18, année 2011, p : 7 et 8.

Il va sans dire que certaines des infractions prévues par le code pénal marocain peuvent être retenues dans l'environnement numérique. Il en est ainsi de l'escroquerie qui peut être commise par le biais de l'ordinateur où à travers le Net. Toutefois, il est juridiquement impossible de retenir le vol d'un fichier informatique si l'acte d'usurpation a consisté dans l'établissement d'une copie, tout en maintenant le fichier original sur le disque dur. Cet exemple dénote de l'inadaptation du dispositif pénal marocain à réprimer des infractions commises par le biais du numérique, en raison de l'absence des textes légaux. En d'autres termes, l'obstacle à l'extension des règles pénales à des actes commis par le biais

de l'ordinateur ou à l'encontre de l'ordinateur réside dans l'absence de l'élément légal nécessaire pour ériger un acte en infraction.[66]

2-2. Règles d'ordre particulier

Ces règles spécifiques s'inscrivent dans une perspective considérant la cybercriminalité comme étant un phénomène spécifique. Cette démarche a abouti à l'adoption de trois textes législatifs[67] d'une grande importance :

- ✓ La loi n°07-03 complétant le code pénal en ce qui concerne les infractions relatives aux systèmes de traitement automatisé des données;
- ✓ La loi n°53-05 relative à l'échange électronique de données juridiques;
- ✓ La loi n°09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.

[66] RMAIL. B, Criminalité informatique ou liée aux nouvelles technologies de l'information et de communication, p 244, op.cit

[67] Signalons par ailleurs, comme cela est de coutume, en particulier lorsqu'il s'agit de domaines liés aux nouvelles technologies, les rédacteurs de ces lois se sont contentés de reproduire presque littéralement les dispositions de la loi française. Il s'agit notamment des lois suivantes :

-La loi n°2004-801 du 6 août 2004, qui modifie la loi du 06 janvier 1978 relative à l'informatique, aux fichiers et libertés ;

-La loi du 5 janvier 1988 dite Loi Godfrain ;

-La loi n°2000-230 du 13 Mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique.

A coté des ces lois, d'autres textes régissaient les infractions informatiques existent déjà à savoir : les règles relatives aux infractions et sanctions ayant trait au secteur de télécommunication, les règles ayant trait aux infractions et sanction en matière de propriété intellectuelles, et les règles en matière de Terrorisme.

2-2-1. La loi n°07-03 complétant le code pénal en ce qui concerne les infractions relatives aux systèmes de traitement automatisé des données

Jusqu'à octobre 2003, le phénomène de la cybercriminalité au Maroc n'a fait l'objet d'aucune disposition législative visant à le réprimer. Il s'agissait encore d'un phénomène mal connu et marginal. Par conséquent, l'arsenal juridique marocain disposait de lacunes sérieuses empêchant la répression des infractions liées à la criminalité informatique. De nombreuses dispositions du code pénal se révèlent parfaitement inadaptées aux spécificités du phénomène. Face à cette situation, le législateur marocain se trouvait contraint d'enrichir le code pénal par des dispositions susceptibles de s'appliquer aux infractions commises par voie informatique ou électronique. C'est ainsi que la loi n°07-03 complétant le code pénal en ce qui concerne les infractions relatives aux systèmes de traitement automatisé des données a vu le jour en 2003. Reproduite à partir de la loi française du 5 janvier 1988 dite loi Godfrain, la loi n°07-03 constitue un texte fondateur pour la mise à niveau de l'arsenal juridique marocain afin de tenir compte des infractions imputables à la criminalité informatique. Elle traite les atteintes aux systèmes de traitement automatisé des données (STAD) et réprime pénalement de nombreux comportements. Les intrusions ainsi que les atteintes aux systèmes de traitement automatisé des données demeurent les plus importantes incriminations contenues dans cette loi.

A. Les intrusions

La loi n°07-03 permet de sanctionner toutes les intrusions non autorisées dans un système de traitement automatisé de données. Elle fait la distinction entre l'accès et le maintien frauduleux dans un STAD. En effet, deux types d'accès illicites peuvent être envisagés :

- L'accès dans l'espace, qui consiste à pénétrer par effraction dans un système informatique (accès frauduleux) ;
- L'accès dans le temps, qui s'agit du fait d'outrepasser une autorisation d'accès donnée pour un temps déterminé (maintien frauduleux).

Les sanctions prévues varient selon que l'intrusion a eu ou non une incidence sur le système en cause.

➢ *L'accès frauduleux dans un STAD*[68]

Parmi les actes réprimés dans la loi n°07-03, on trouve en premier lieu l'accès frauduleux. Cette infraction résulte de l'article 607-3 du code pénal qui dispose dans sa rédaction de 2003 : « le fait d'accéder, frauduleusement, dans tout ou partie d'un système de traitement automatisé des données est puni d'un mois à trois mois d'emprisonnement et de 2.000 à 10.000 dirhams ou de l'une de ces deux peines seulement ». Dès lors que le maintien ou l'accès frauduleux entraîne une altération du système, la loi marocaine prévoit un doublement de la peine[69]. L'accès au STAD peut se faire

- Depuis l'extérieur du système : ainsi, un pirate qui pénètre dans un ordinateur connecté à l'internet tombe sous le coup de la loi.

[68] Il convient ainsi, de préciser que l'accès frauduleux à un STAD, tel qu'il a été précisé par la jurisprudence française, est constitué « *dès lors qu'une personne, non habilitée, pénètre dans ce système tout en sachant être dépourvue d'autorisation, peu importe le mobile* ». Ce qui recouvre un grand nombre d'hypothèses. Dans cette perspective, la Cour d'appel de Paris a considéré dans un arrêt du 5 avril 1994 que « l'accès frauduleux, au sens de la loi, vise tous les modes de pénétration irréguliers d'un système de traitement automatisé de données, que l'accédant travaille déjà sur la même machine mais à un autre système, qu'il procède à distance ou qu'il se branche sur une ligne de communication

[69] En effet, l'article 607-3, al. 3 du Code pénal dispose « La peine est portée au double lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le STAD, soit une altération du fonctionnement de ce système

- Depuis l'intérieur du système : un salarié qui, depuis son poste, pénètre dans une zone du réseau de l'entreprise à laquelle il n'a pas le droit d'accéder pourra être poursuivi.

➢ *Le maintien frauduleux dans un STAD*

La loi marocaine incrimine également le maintien frauduleux dans un système de traitement automatisé de données. L'article 607-3 du code pénal marocain dispose : « Est passible de la même peine toute personne qui se maintient dans tout ou partie d'un système de traitement automatisé de données auquel elle a accédé par erreur et alors qu'elle n'en a pas le droit ».

B. Les atteintes

Les atteintes au STAD ont tendance à devenir de plus en plus fréquentes de nos jours, que le but soit le simple vandalisme ou bien encore, de façon plus élaborée, un but économique (vol ou altération de données dans le but d'en retirer de l'argent). Le législateur marocain a prévu des incriminations de ces délits dans le cadre de la loi n°07-03.

➢ *Les atteintes au fonctionnement d'un STAD*

L'atteinte au fonctionnement d'un STAD peut être constitué de manières très diverses, par tout comportement ou toute action qui va entraîner temporairement ou de manière permanente une gêne dans le fonctionnement du système, une dégradation du système voire le rendre totalement inutilisable. L'article 607-5 du Code pénal, inséré en vertu de la loi n°07-03, dispose que « Le fait d'entraver ou de fausser intentionnellement le fonctionnement d'un système de traitement automatisé des données est puni d'un an à trois ans d'emprisonnement et de 10.000 à 200.000 dirhams d'amende ou de l'une de ces deux peines seulement ».

A la lecture de l'article 607-5, il ressort que l'élément matériel d'une atteinte portée à un STAD lui-même et non pas à ses données peut provenir de

l'entrave ou du faussement de ce dernier. L'exemple le plus connu de ce délit est l'attaque par déni de service[70].

- *Les atteintes aux données*[71]

En réalité, toute manipulation de données, qu'il s'agisse de les introduire, de les supprimer, de les modifier ou de les maquiller, provoque, en toutes circonstances, une altération du système. Le fait de modifier les tables d'une base de données, de déréférencer l'adresse d'un serveur Web dans les moteurs de recherche, ou encore, de défacer un site web pour y insérer une image indécente, constituent autant d'atteintes visées par le texte.

Si dans le cadre de la législation française, le délit n'est constitué que si les atteintes sont réalisées avec une intention délictueuse et hors de l'usage autorisé, il convient d'observer à propos de cet élément intentionnel une des rares dispositions que le législateur marocain n'a pas « empruntée » à la loi Godfrain. Il s'agit en l'occurrence de l'exigence que l'atteinte soit commise « *aux mépris des droits d'autrui* ».

Enfin, il convient de signaler que pour tous ces délits, que ce soit pour les intrusions (accès et atteinte frauduleux au STAD) et pour les atteintes (atteintes au fonctionnement et atteintes aux données d'un STAD), la tentative est punie des mêmes peines[72].

2-2-2. La loi 53-05 relative à l'échange électronique de données juridiques

Cette réforme a pour objet de fixer le régime applicable aux données juridiques échangées par voie électronique, à l'équivalence des documents établis sur papier et sur support électronique et à la signature électronique. Elle détermine également le cadre juridique applicable aux opérations effectuées par

[70] Voire chapitre 1 section 3
[71] Voir article 607-6
[72] En effet, l'article 607-8 du code pénal dispose « *La tentative des délits prévus par les articles 607-3 à 607-7 ci-dessus et par l'article 607-10 ci-après est punie des mêmes peines que le délit lui-même* »

les prestataires de services de certification électronique, ainsi que les règles à respecter par ces derniers et les titulaires des certificats électroniques délivrés. En outre, la loi institue une autorité nationale d'agrément et de surveillance de la certification.

A. La preuve

La loi n°53-05 comporte deux volets particulièrement novateurs en matière de preuve. Il s'agit de la redéfinition de la preuve littérale et la consécration de la force probante de l'écrit électronique.

- *La redéfinition de la preuve littérale*

La loi n°53-05 relative à l'échange électronique de données juridiques a pris soin de modifier la formulation de l'article 417, alinéa 2 du Dahir des Obligations et Contrats (D.O.C). L'article 417, alinéa 2 dispose que la preuve littérale peut également résulter « *de tous autres signes ou symboles dotés d'une signification intelligible quels que soient leur support et leurs modalités de transmission* ». Le législateur affirme donc l'équivalence entre le papier et l'électronique. Cela a constitué une avancée fondamentale du droit de la preuve. La définition respecte ainsi le principe de neutralité technologique. La seule condition posée réside dans le fait que le message doit être intelligible, c'est-à-dire qu'il s'agisse d'une information destinée à être communiquée et comprise.

- *La consécration de la force probante de l'écrit électronique*

La redéfinition de la preuve littérale n'est pas le seul apport de la nouvelle loi, la consécration de la force probante de l'écrit électronique est aussi l'un des volets particulièrement novateurs de la loi n°53-05. En effet, cette loi confère la même force probante à l'écrit électronique que l'écrit sous forme papier, à condition qu'il permette à la personne dont il émane d'être dûment identifiée et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité[73].

[73] L'article 417-1 dispose que « *l'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse dûment être identifiée à la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité* ».

B. La signature électronique

Dans le but de faciliter l'utilisation des signatures électroniques, de contribuer à leur reconnaissance juridique et d'instituer un cadre juridique pour les services de certification, la loi n°53-05 reconnaît la validité juridique de la signature électronique dés lors qu'elle remplira certaines conditions. Cette reconnaissance constitue une avancée importante pour la promotion du commerce électronique. Elle en est même son fondement de base.

- *La reconnaissance juridique de la signature électronique*

Le texte de la loi n°53-05 non seulement reconnaît juridiquement la signature électronique, mais il va encore plus loin en consacrant la validité de la signature électronique en l'absence de toute convention préalable. Cependant, la signature électronique ne peut être qualifiée de valide tant qu'elle ne remplisse pas certaines conditions. En effet, l'article 417-2, dispose que lorsque la signature est électronique, « il convient d'utiliser un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache ».

Dans l'absolu, la signature remplit deux fonctions juridiques de base. Il s'agit de l'identification de l'auteur et de la manifestation de sa volonté d'approbation du contenu de l'acte. Il va de même pour la signature électronique. L'article précité exige que le procédé d'identification soit d'une part, fiable et d'autre part, il doit garantir le lien de la signature électronique avec l'acte, lien qui en effet indispensable pour que la signature électronique joue pleinement sa fonction d'approbation du contenu de l'acte.

La fiabilité de ce procédé est présumée, jusqu'à preuve de contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, conformément à la législation et la réglementation en vigueur en la matière[74].

[74] L'article 417-3 dispose que « la fiabilité d'un procédé de signature électronique est présumée, jusqu'à preuve de contraire, lorsque ce procédé met en œuvre une signature électronique sécurisée ».

Pour qu'elle puisse être qualifiée de « sécurisée », la signature électronique doit remplir les conditions suivantes:

- Elle doit être propre au signataire ;
- Elle doit être créée par des moyens que le signataire puisse garder sous son contrôle exclusif ;
- Elle doit garantir avec l'acte auquel elle s'attache un lien tel que toute modification ultérieure dudit acte soit détectable ;
- Elle doit être produite par un dispositif de création de signature électronique, attestée par un certificat de conformité ;

Les données de vérification de la signature électronique sécurisée doivent être mentionnées dans le certificat électronique sécurisé prévu à l'article 10 de la présente loi.

2-2-3. La loi n°09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel[75]

La loi n° 09-08 s'applique au traitement des données à caractère personnel, sous quelque forme que ce soit relatives à une personne physique identifiée ou identifiable .Le nom, prénom, adresse, courriel, photographie d'identité, numéro d'identification, empreintes digitales constituent par exemple des données à caractère personnel. Dans cette optique peut-on considérer une adresse IP comme une donnée à caractère personnel et par conséquent tombe sous la protection de la loi n°09-08.

Le traitement qui fait l'objet de la protection des données à caractère personnel concerne toute opération ou tout ensemble d'opérations portant sur des données à caractère personnel réalisés ou non par le biais de procédés automatisés. Il s'agit notamment de la collecte, l'enregistrement, l'organisation,

[75] Inspirée de la célèbre loi française Informatique et Libertés, la loi n° 09-08 relative à la protection des personnes physiques à l'égard des traitements des données à caractère personnel a été publiée au Bulletin Officiel n° 5744 du 18 Juin 2009, après avoir été promulguée par le Décret n° 2-09-165, en date du 21 mai 2009. Elle introduit, pour la première fois, dans le paysage juridique marocain, un ensemble de dispositions légales harmonisées avec le droit européen et, notamment, avec la Directive Communautaire n° 95/46

la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction. Rappelons, par ailleurs, qu'une seule de ces opérations suffit à constituer un traitement de données à caractère personnel qui sera soumis aux dispositions de la loi n°09-08. Le simple fait de collecter les données, sans même les communiquer ou les diffuser, suffit à caractériser un traitement[76].

Il convient de souligner par ailleurs que les implications de cette nouvelle loi concernent non seulement les entreprises et les citoyens établis sur le territoire marocain mais aussi toutes les entreprises étrangères qui entretiennent des relations d'affaires avec leurs homologues marocaines ou qui échangent des données avec leurs filiales ou leurs maisons mères marocaines, tout en utilisant des moyens situés sur le territoire marocain. Toutefois, le champ d'application de cette loi exclut les données relatives à l'exercice d'activités personnelles ou ménagères, celles obtenues au service de la Défense nationale et de la Sûreté intérieure et extérieure de l'Etat, ou encore celles obtenue dans le cadre du traitement effectué en application d'une législation particulière.

Chaque traitement de données à caractère personnel, ou son transfert à des tiers, nécessite en principe, pour être effectué, le consentement indubitable de la personne concernée par ledit traitement ou ledit transfert. Toutefois, ledit consentement n'est pas requis dans certains cas, notamment pour le respect d'une obligation légale, la sauvegarde d'intérêts vitaux ou l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique.

2-2-4. Règles relatives au secteur de Télécommunication[77]

[76] QUEMENER.M, FERRY. J, « Cybercriminalité : Défi mondial » Edition Economica 2009, Page 106

[77] Dahir n°1-97-162 du 7/08/1997 portant promulgation de la loi n°24-97 relative à la Poste et aux Télécommunication, tel que modifié par le Dahir n°1-01-123 du 29/06/2001 portant promulgation de la loi n°79-

Plusieurs lois ont été promulguées dans le but d'incriminer et sanctionner les actes illicites en matière de Télécommunication. Les infractions prévues par ces lois pourront être constatées par des procès-verbaux dressés par des officiers de police judiciaire et les agents de la force publique. Ainsi que par les employés assermentés et commissionnés à cette fin par l'ANRT.

L'ANRT pourra prendre immédiatement et auprès du contrevenant toutes les mesures provisoires et urgentes qui seraient indispensables pour faire cesser les dommages résultant des infractions.

2-2-5. Règles relatives à la propriété intellectuelle

Selon le Dahir n°1-00-20 du 15/02/2000 portant promulgation de la loi n°2-00 relative aux droit d'auteur et droits voisins et le Dahir modificatif n°1-05-192 du 14/02/2006 portant promulgation de la loi n°34-1-05, il est institué un certain nombre d'infraction auxquelles plusieurs sanction ont été réservées.

Ces infractions de plus en plus perpétrées avec grande facilité dans l'environnement numérique, en raison de la sophistication des moyens utilisés, se présentent comme suit :

- Toute violation d'un droit protégé en vertu de la loi sur les droit d'auteurs, si elle est commise intentionnellement ou par négligence et dans le but lucratif, expose son auteur aux peines prévues dans le code pénal. Le montant de l'amende est fixé par le tribunal, compte tenu des gains que le défendeur a retirés de la violation ;
- Les actes suivants sont considérés comme illicites et, aux fins des articles 61 à 63 de la loi sur les droit d'auteur, sont assimilés à une violation des droits d'auteur et autres titulaires du droit d'auteurs ;
    - La suppression ou modification, sans y être habilité, de toute information relative au régime des droits se présentant sous forme électronique ;

99, le Dahir n°1-04-154 du 04/11/2004 portant promulgation de la loi n°55-01 et le Dahir n°1-07-43 du 17/04/2007 portant promulgation de la loi n°29-06.

- La distribution ou l'importation aux fins de distribution, la radiodiffusion, la communication au public ou la mise à disposition du public, sans y être habilité, d'œuvre d'interprétations ou exécution, de phonogrammes ou d'émissions de radiodiffusions, en sachant que des informations relatives au régime des droits se présentant sous formes électronique ont été supprimées ou modifiées sans autorisations ;

En outre , selon la dernière réforme du texte sur les droits d'auteur opérée par la loi n°34-05 modifiant et complétant la loi n°2-00 relative aux droit d'auteurs et droit voisins , les prestataires de certains services en ligne peuvent être rendus responsables pénalement des violations des droits d'auteurs.

2-2-6. Règles relatives au cyberterrorisme

Selon la loi n°03-03 relative à la lutte contre le terrorisme[78], les infractions informatiques ou liées aux NTIC sont des actes terroristes, lorsqu'elles sont commises dans les conditions prévues par l'article 218-1 dudit texte.

Selon l'article susvisé, les infractions informatiques ou liées aux NTIC sont des actes de terrorisme, dès lors qu'elles sont intentionnellement commises en relation avec une entreprise individuelle ou collective ayant pour but de troubler gravement l'ordre public par l'intimidation, la terreur ou la violence.

Section 3 : le Maroc et le défi de la confiance numérique

Tout comme la criminalité traditionnelle et sa structuration à travers le crime international organisé, il appartient à l'état de droit de garantir la sécurité dans le cyberespace et d'établir une confiance numérique, seuls éléments

[78] Promulguée par le Dahir n° 1-03-140 du 26 Rabiaa 1424

capables de favoriser le développement des nouvelles économies basées sur la dématérialisation des relations et des échanges[79].

La tache est plus ardue, et les mesures prises se diffèrent d'un pays à l'autre et selon les cultures locales. En effet, par exemple les Etats -Unis inscrivent leur politique de répression contre la cybercriminalité dans le cadre de la protection des intérêts vitaux de la nation américaine, en France, la lutte s'inscrit dans une perspective de protection des libertés individuelles et de droit de l'homme.

Concernant le Maroc, en l'absence d'une stratégie décrivant la stratégie tout comme la vision globale à mettre en place pour sécuriser le cyberespace marocain, nos politiques ont entrepris différentes actions à plus ou moins grande échelle. Mais parmi tous ces initiatives, le programme « confiance numérique » qui entre dans le cadre de la stratégie « Maroc numérique 2103 » demeure la feuille de route la mieux élaborée à l'heure actuelles. C'est la raison pour laquelle nous avons jugé nécessaire de présenter d'abord les piliers de la confiance numérique(1) et après nous procéderons à une étude de programme de confiance numérique marocain avec tous ses difficultés et ses insuffisances (2).

1- Les piliers de la confiance numérique

La confiance numérique dans tout pays a quatre piliers à savoir :

- ✓ La garantie de l'intégrité du réseau et de la qualité du service ;
- ✓ La protection de la vie privée et des données personnelles ;
- ✓ La protection des mineurs ;
- ✓ La prévention de la piraterie et du vol.

1-1. La garantie de l'intégrité du réseau et de la qualité du service

[79] FRANCHIN. F, MONNET. R, « le Business de la Cybercriminalité », p 55, Hermes Science publication, collection Management et informatique, 2005

pour les consommateurs et les entreprises, dans la mesure où ceci est lié à la protection des plateformes technologiques contre toutes attaques criminelles portant atteinte à la sécurité, en vue de garantir une connectivité Internet optimale malgré les surcharges de trafic ou les attaques criminelles externes, en vue de sécuriser l'environnement informatique pour les consommateurs individuels comme pour les entreprises contre toutes perturbations dues à des virus ou autres logiciels malveillants.

1-2. La protection de la vie privée et des données personnelles

Autrement dit protéger les données électroniques privées des consommateurs (identité, mots de passe, profils d'usage et de consommation, etc.) contre l'accès illicite, la publication ou l'exploitation commerciale sans consentement, et prévenir le vol d'identité et la fraude.

1-3. La protection des mineurs

C'est-à-dire protéger les enfants de toute exposition à des contenus indésirables, empêcher le harcèlement et tout autre comportement hostile, empêcher le grooming (c.-à-d. l'utilisation de sites de rencontres en ligne par des adultes cherchant à séduire des mineurs) ou toute autre forme de sollicitation d'enfants par des adultes et lutter contre les contenus de pornographie enfantine.

1-4. La prévention de la piraterie et du vol

Enrayer le vol de contenus protégés par des droits d'auteur et sécuriser les transactions e-commerce pour toutes les parties engagées. L'industrie a besoin d'agir de manière proactive sur la base d'une vision holistique de toutes ces questions. Cette approche se retrouve dans le concept de « Confiance Numérique». Promouvoir la Confiance Numérique dépasse largement la simple observation des prescriptions légales cela devient presque un préalable commercial et l'équivalent d'un permis d'agir. Comme certaines études de cas le montreront, l'observation des prescriptions légales ne permet pas à elle seule d'obtenir l'acceptation du consommateur. Les politiques des opérateurs et les pratiques commerciales se doivent d'aborder tous les questions légales,

économiques et publiques associés à ces domaines de manière conjointe et cohérente, afin de permettre la prochaine phase de croissance de l'économie numérique.

2- Confiance numérique au Maroc et les difficultés enregistrées

Le développement des TI ne peut avoir lieu sans instaurer les conditions de la confiance numérique. C'est le constat de base de « Maroc Numérique » en ce qui concerne la SSI (sécurité des systèmes d'information). Le Maroc alors a opté pour une stratégie de confiance numérique basée sur trois initiatives qu'on va les détailler après. Toutefois, les efforts fournis dans ce cadre souffrent encore de plusieurs limites et obstacles, chose qui pourra entraver le processus de confiance en ligne.

2-1. La stratégie marocaine de confiance numérique

La stratégie marocaine de confiance numérique s'articule autours trois initiatives clés :

- ✓ Initiative 1 : renforcement du cadre législatif ;
- ✓ Initiative 2 : mettre en place les structures organisationnelles appropriées ;
- ✓ Initiative 3 : promouvoir et sensibiliser les acteurs de la société à la sécurité des systèmes d'information

2-2-1. Renforcement de cadre législatif

Pour faire face à la cybercriminalité, le Maroc a renforcé sans cadre législatif avec trois lois[80] qui ont mis à niveau l'arsenal juridique marocain à savoir :

- La loi n°07-03 complétant le code pénal en ce qui concerne les infractions relatives aux systèmes de traitement automatisé des données ;
- La loi n°09-08 relative à la protection des personnes physique à l'égard du traitement des données à caractère personnel ;

[80] Voir section 2 chapitre 2

- La loi n° 53-05 relative à l'échange électronique des données juridiques.

La promulgation de ces trois lois a contribué fortement à la protection des personnes physiques à l'égard du traitement de données à caractère personnel, comme elle a favorisé la dématérialisation des transactions électroniques

2-2-2. Mise en place des structures organisationnelles appropriées

Les ripostes juridiques en matière de lutte contre la cybercriminalité, aussi exhaustives soient-elles, seront insuffisantes si elles ne sont pas accompagnées par la mise en place d'institutions chargées notamment de la répression, d'investigation et de veille en matière de cybercriminalité. Dans cette perspective, le programme « confiance numérique » a eu le mérite de prévoir la mise en place des organismes suivants :

- ✓ Le Comité de la Sécurité des Systèmes d'Information (SSI) ;

L'organisme ma-CERT ;

- ✓ L'organisme de tiers de confiance ;
- ✓ La commission Nationale de Protection des Données Personnelles (CNDP) ;
- ✓ Les sites de back-up.

A. Le Comité de la Sécurité des Systèmes d'Information (SSI)

Faire de la sécurité informatique revient à être fermé dans un environnement complètement ouvert. A cet effet, il est prévu dans le cadre du « Maroc Numérique 2013 » de mettre en place un comité de la sécurité des systèmes d'information. Il aura notamment comme mission, l'élaboration de la politique relative à la protection des infrastructures critiques du Royaume[81].

B. Mettre en place le Centre Marocain d'Alerte et de Gestion des Incidents Informatique (ma-Cert)

[81] Conformément à l'article 9 de décret n°2-08-444 du 25 joumada 1430 (21 mai 2009) instituant le conseil national des technologies de l'information et de l'économie numérique dispose que « Le Conseil national peut créer en son sein tous autres comités spécialisés qu'il estime nécessaires à l'accomplissement de ses missions»

S'inscrivant dans le cadre du plan "Maroc Numérique 2013″, l'objectif du centre est de mettre en place un processus de surveillance et de traitement d'incidents relatifs à la sécurité des systèmes d'information des organismes publiques. MA-CERT aura pour missions : la surveillance et la coordination des systèmes de sécurité informatique au niveau national. Le traitement des incidents liés à la sécurité des SI, notamment les cyber-attaques. La prévention et la proposition de solutions de lutte contre les menaces d'usurpation, de vol, ou de corruption de donnée. L'analyse et la restauration des systèmes attaqués/infectés.

C. Mettre en place un Tiers de confiance

Réfléchissant aux métiers de tiers de confiance, Alain Borghesi et Arnaud Belleil en proposaient en 2006 une définition large : "*un acteur, agissant dans l'univers des nouvelles technologies, se portant garant dans une transaction ou un échange entre deux parties entre lesquelles la confiance réciproque ne va pas forcément de soi*".

Au Maroc, Conformément à la loi n°53-05 et à son décret d'application, et afin de mettre en pratique les différentes dispositions relatives à la délivrance de certificats électroniques, Poste Maroc a été choisi pour jouer le rôle de tiers de confiance. Le but, c'est d'offrir aux échanges électroniques une garantie de fiabilité, d'authentification et d'intégrité des données et ceci par l'émission et la délivrance de certificats électroniques. L'ANRT est considérée aussi comme autorité nationale d'agrément et de surveillance de la certification électronique.

- *La commission nationale de la protection des données personnelles*

Pour veiller, au respect de ses différentes dispositions, la loi 09-08 a institué la Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel. Chargée de veiller à la mise en œuvre des dispositions de la loi, la commission nationale est un organe doté de prérogatives et de larges pouvoirs d'investigation, de contrôle et d'intervention. Ses membres sont nommés par Sa

Majesté le Roi afin de garantir leur autonomie et leur impartialité vis-à-vis des différentes parties prenantes[82].

D. Mettre en place deux instances au sein de la direction de la défense nationale

Au Journal officiel du 17 octobre 2011, est paru le Décret n° 2.11.508 portant création de la Commission Stratégique de la Sécurité des Systèmes d'Information et le Décret n° 2.11.509 portant création d'une Direction Générale de la Sécurité des Systèmes d'Information. Les deux instances seront créées au sein de la direction de défense nationale[83].

2-2-3. Promotion d'une culture de sécurité

Le Maroc, est dans le but de promouvoir une culture de sécurité, s'est engagé à :

- ✓ Mettre en œuvre un programme de sensibilisation et de communication sur la SSI ;
- ✓ Mettre en place des formations sur la SSI à destination des élèves ingénieurs
- ✓ Mettre en place des formations à destination des professions juridiques ;
- ✓ Définir une charte des sites marchands.

A. Mettre en œuvre un programme de sensibilisation et de communication sur la SSI

Plusieurs actions de sensibilisation doivent être envisagées, à titre d'exemple :

- ➢ Inciter les associations qui œuvrent dans le domaine des enfants à s'intéresser davantage à la sensibilisation en matière des dangers de l'internet dont sont victimes les jeunes et les enfants
- ➢ Obliger les cybercafés à aménager des salles destinées aux mineurs, dotées d'ordinateurs utilisant des logiciels de protection.

[82] Le décret d'application de la loi 09-08 a été publié au Bulletin Officiel N° 5744 dans son édition du 18 juin 2009. Ledit décret a fixé notamment les conditions et modalités de désignation des membres de la Commission Nationale, ses règles de fonctionnement et ses pouvoirs d'investigation, ainsi que les conditions de transfert des données à caractère personnel vers un pays étranger

[83] Voir Bulletin Officiel dans l'annexe

- Former des cadres sur la méthode de sensibilisation dans les milieux de l'enseignement, des jeunes, de l'enfance et de la famille pour mener des campagnes au sein des écoles, des campings et des maisons de jeunes.

B. Mettre en place des formations sur la SSI à destination des élèves ingénieurs

La promotion de la culture de sécurité passe aussi par la mise en place des formations à destination des étudiants de l'enseignement supérieur. En effet, face à la demande accrue des organisations publiques et privés en terme de personnels qualifiés et spécialisés en sécurité SI, il est devenu extrêmement urgent de proposer des formations spécialisées en SSI à destination des étudiants.

C. Mettre en place des formations à destination des professions juridiques

Des passerelles entre l'univers informatique et celui des juristes comprenant aussi bien des avocats, des magistrats que des policiers et des gendarmes. Concernant la formation des juristes, plusieurs ateliers ont eu lieu. Le dernier était organisé par Microsoft en partenariat avec le ministère de la Justice. Cette initiative a pour but :

- ✓ Soutenir le monde juridique dans la lutte contre le piratage
- ✓ Une sensibilisation des juristes à l'importance de la propriété intellectuelle[84].

De cette formation, il ne faut pas oublier les cyberenquêteurs. Qu'ils soient issus de la police ou de la gendarmerie, leurs sensibilisations à la lutte contre la cybercriminalité par le biais d'une formation spécifique est indispensable.

D. Définir une charte des sites marchands

[84] http://www.microsoft.com/northafrica/press/Pages/Article.aspx?id=49 consulté le 18/6/2012

Pour pouvoir renforcer la confiance des citoyens dans le commerce électronique, l'Etat s'est engagé dans le cadre de la stratégie « Maroc Numérique 2013 » à mettre en place une charte des sites marchands. Constituée à partir des meilleures pratiques en termes de sécurisation des sites de commerce électronique, cette charte permettra aux cyberconsommateurs de mieux qualifier le respect des exigences de sécurité par les différents sites. Le respect de la charte donnera lieu à un label qui sera mis en place en partenariat avec les fédérations notamment la CGEM[85].

2-2. Ratification des conventions internationales sur la cybercriminalité

Tout effort de lutter individuellement contre ce danger mondialisé de cybercriminalité est un effort voué à l'échec. Conscient de ce constat, le Royaume a opté, à coté des efforts à l'échelle nationale, de coopérer à l'international, et ce par le biais de ratification notamment, de la convention de Budapest et la convention arabe, les deux ayant trait à la lutte contre la cybercriminalité.

Concernant la convention de Budapest sur la cybercriminalité, elle est le premier texte international à se pencher sur ce nouveau fléau.

La Convention traite en particulier des infractions portant atteinte aux droits d'auteur, de la fraude liée à l'informatique, de la pornographie enfantine, ainsi que des infractions liées à la sécurité des réseaux. Elle contient également une série de compétences procédurales, tels que la perquisition de réseaux informatiques et l'interception.

Son principal objectif, énoncé dans le préambule, est de poursuivre "une politique pénale commune destinée à protéger la société contre la cybercriminalité, notamment par l'adoption d'une législation appropriée et la stimulation de la coopération internationale".

[85] ELAZZOUZI. A, « la Cybercriminalité au Maroc », p149, op.cit

Elle sera complétée par un Protocole additionnel visant la criminalisation de la diffusion de propagande raciste et xénophobe par le biais des réseaux informatiques dont l'élaboration débutera en décembre 2001.

S'agissant de la Convention arabe de lutte contre la cybercriminalité, elle vise à promouvoir et à renforcer la coopération entre les pays arabes en la matière dans la perspective de contenir les dangers de ce phénomène et de préserver la sécurité des Etats arabes. Elle s'applique, entre autres, aux crimes relatifs aux technologies de l'information, notamment ceux concernant la modification ou la destruction des données stockées et des dispositifs et systèmes électroniques et les réseaux de télécommunication ainsi que les dommages subis par les utilisateurs et les bénéficiaires et l'accès aux informations secrètes du gouvernement.
Elle porte également sur les aspects liés au mauvais usage des technologies de l'information et de production, ainsi qu'à la lutte contre la cybercriminalité et le cyber-terrorisme.

2-3. La confiance numérique au Maroc : un long travail à faire

Certes, le Royaume s'est engagé dans plusieurs réformes afin de lutter contre la cybercriminalité et rendre les internautes marocains plus protégés sur la toile d'Internet où tous a droit d'y accéder. Or, ces efforts demeurent limités par rapport à d'autres pays comme la France et les Etats-Unis, et ce pour plusieurs raisons que nous allons détailler.

2-3-1. les Marocains encore peu confiant au commerce en ligne

Certes, le e-commerce s'impose par son accessibilité et sa fluidité dans les transactions commerciales, mais la structuration et le développement de la confiance des consommateurs sont des éléments à renforcer pour améliorer la compétitivité des entreprises opérantes sur le net. Le facteur psychologique et culturel constitue la cause principale à la réticence constatée chez le consommateur marocain pour ce qui est de l'e-paiement, puisque plus de 72% des internautes ont un manque de confiance vis-à-vis des sites électroniques

(sécurité de paiement, délais de livraison, qualité des produits, traitement des données personnelles). Le Maroc reste une société de cash, ce qui pose de sérieux freins au développement du e-commerce au Maroc, où juste 12% des cartes bancaires sont utilisées dans le paiement en ligne. Le faible taux de bancarisation, le retard en matière de développement du paiement par carte bancaire sur internet, la crainte de s'engager dans ce nouveau mode d'achat peu maîtrisé, sont autant de facteurs qui empêchent le développement de ce secteur. Le côté immatériel du e-commerce peut, en effet, dissuader certains consommateurs habitués à voir et à toucher le produit avant de décider son acquisition. Pour y remédier, la sensibilisation et la communication s'imposent, à côté de la mise en place d'un cadre législatif et réglementaire.

2-3-2. Un arsenal juridique moins sévère

Il est certain que les textes marocains[86] viennent combler en partie une grande lacune dans la législation pénale nationale, dans la mesure où ils érigent en infractions pénales des comportements informatiques ou liés aux TIC, qui échappaient à toutes sanctions, en dépit de leur dangerosité pour la vie privée, pour l'économie nationale et pour la sécurité.

Toutefois, malgré ces apports appréciables, il n'en demeure pas moins vrai que cet arsenal peut se prêter à la critique sur plusieurs plans : il se montre moins relativement moins sévère que des textes étrangers en la matière, notamment le texte français et accuse quelques insuffisances quant aux actes quant aux actes qu'il incrimine (on parle surtout de la loi n°09-08).

A. Manque de sévérité du texte marocain

Par caractère moins élevé des sanctions prévues par le texte marocain, il ya lieu d'entendre les quanta des peines, tels que fixés par les textes dédiés aux

[86] Voir section 2 chapitre 2

atteints aux systèmes de traitement automatisé des données, indépendamment de tout autre texte, ainsi que de toute individualisation judiciaire des peines[87].

Quant aux sanctions complémentaires, une différence notable est à relever entre le nouveau texte marocain et le texte français. En réalité, le législateur s'est montré restrictif quant aux sanctions complémentaires, dans la mesure où il n'a pas prévu la possibilité de condamner les auteurs des faits prévus dans les différents articles du texte à :

- L'interdiction d'exercer l'activité professionnelle ou sociale dans l'exercice de laquelle ou l'occasion de l'infraction a été commise ;
- La fermeture pour une durée de 5 ans au plus, des établissements de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre des faits incriminés ;
- L'exclusion, pour une durée de 5 ans au plus, des marchés publics ;
- L'interdiction, pour une durée de 5 ans au plus d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés.

Il ressort du texte marocain encore que le législateur se montre moins sévère dans la mesure où il n'impose pas, à la différence de son homologue français, le prononcé en même temps des peines privatives de liberté et des amendes.

B. Les insuffisances du texte marocain quant aux actes incriminés

Une simple lecture du texte marocain permet de conclure qu'un certain nombre d'actes n'ont pas été appréhendés par la loi. A ce titre, il est possible de souligner tout particulièrement le vide marquant le texte marocain concernant la récupération des données dans les systèmes de traitement automatisé des données en dehors de tous les actes spécifiés dans ce texte[88].

[87] Voir tableau comparatif (sanctions en droit marocain et en droit français) dans l'Annexe
[88] RMAIL. R, « Criminalité informatique ou liée au nouvelles technologies de l'information et de communication » ; P 288, 292, 293, op.cit

Conclusion du deuxième chapitre

Conscient de la gravité du phénomène cybercriminel, le Maroc s'est basé sur deux volets pour faire face à ce danger : volet juridique et volet sécurité informatique. Juridiquement le Maroc a promulgué des nouvelles lois relatives aux TIC, tandis qu' au volet de sécurité informatique le Maroc a opté pour la stratégie de « confiance numérique » dont les piliers suscités visent de rendre les internautes marocains plus confiant en ligne. Toutefois, quelques lacunes et obstacles subsistent encore, surtout juridiquement, car le texte marocain en la matière demeure moins sévère et plusieurs actes ne sont pas incriminés. Au niveau de sécurité, les mesures prises n'ont pas pu empêcher les cybercriminels à diminuer leurs tentatives de fraudes informatiques.

La lutte alors contre la cybercriminalité n'est pas question technique seulement mais aussi a trait au degré de formation des utilisateurs, surtout que certains cyberdélits – notamment ceux qui s'apparentent à la fraude, tels que le hameçonnage (phishing) et l'espionnage (spoofing) – ne sont pas liés généralement à une absence de protection technique, mais plutôt à un manque de sensibilisation des victimes.

CONCLUSION

Certes, notre choix de donner une définition pratique de la cybercriminalité était nécessaire dès le début de cette recherche. La définition nécessairement large de la cybercriminalité que nous avons proposée est la suivante : toute action illicite associée à l'interconnexion des systèmes informatiques et des réseaux de télécommunication, où l'absence de cette interconnexion empêche la perpétration de cette action illicite. Cette définition s'applique aux systèmes informatiques, au sens le plus large possible. Même si nous avons pu associer plus étroitement ordinateurs et fraude informatique, le problème de la spécificité serait resté entier.

Dans le chapitre premier, on a aussi indiqué qu'un nombre non moins important d'acteurs dangereux (cyberdélinquants), aux motivations assez diverses, compétitionnent ingénieusement dans le cyberespace, en usant d'une gamme de techniques ou méthodes qui catégorise la cybercriminalité en deux types : infractions dont la cible est l'ordinateurs et infractions dont l'ordinateur est le facilitateur.

Toutes ses formes ont facilité l'appât de gain, les conséquences demeurent couteuses et portent préjudices aux internautes victimes ainsi qu'aux économies des pays.

Les états doivent combattre alors cette menace, techniquement et surtout juridiquement.

Le Maroc, fait parti de ces pays, doit réagir à tout niveau, pour stopper cette menace.

Dans le deuxième chapitre théorique, nous avons essayé de donner une idée sur la réaction du Maroc face à l'explosion du phénomène de la cybercriminalité.

L'adoption de la stratégie de confiance numérique, la mise à niveau de l'arsenal juridique marocain, demeurent les efforts les plus constatés.

Ces réformes surtout juridiques, font objet de plusieurs critiques du fait de leur manque de sévérité, et du fait que plusieurs actes considérés comme infractions numériques n'ont pas été appréhendés par les lois marocaines en la matière, sans oublier que plusieurs actes cybercriminels font encore objet de droit commun.

Il est proposé d'éviter d'alors légiférer par saupoudrages d'articles à l'intérieur de textes disparates très anciens. Pourquoi pas un code juridique global sur Internet.

In fine, un projet de loi sur la cybercriminalité est en cours de discussion au parlement. C'est après son acceptation et son entrée en vigueur, qu'on pourra parler d'un arsenal juridique fort apte de sécuriser les internautes marocains, contre tout danger cybercriminel.

BIBLIOGRAPHIE

OUVRAGES

- AMBRIOSI .A, PEUGEOT .V, PIMIENTA .D *« Enjeux de mots : regard sur les sociétés de l'information »*,2005. C et F édition.

-CHAWKI Mohammed, « *Essai sur la notion de cybercriminalité* », IEHEI, juillet 2006.

-ElAZZOUZI Ali, « *La Cybercriminalité au Maroc* », BISHOPS SOLUTION 2010.

-FILIOL Eric, RICHARD Philipe « *criminalité enquêtes sur les mafias qui envahissent le Web* ». Duond, Paris, 2006.

-FRANCHIN .F, MONNET. R, « *le Business de la Cybercrminalité* », Herms Sciene publication, collection Management et informatique, 2005

-PEUGEOT. V, PIMIENTA. D ***« Enjeux de mots : regard sur les sociétés de l'information »***,2005. C et F édition.

-QUEMENER Meriem, CHARPENEL Yves. « *Cybercriminalité Droit pénal appliqué* », Edition Economica, 2010

-QUMENER Myriam, Ferry Joël, « Cybercriminalité : Défi mondial » Edition Economica 2009

-RMAIL Bouchaib. « *Criminalité informatique ou liée aux nouvelles technologies de l'information et de la communication* ». SOMAGRAM, 2ém édition, 2010

-TOUMLILT Mohammed diyaâ « *le commerce élecrtonique au Maroc : Aspects juridiques* », les éditions maghrébines.

REVUES ET ARTICLES

-BENSGHIR Fouad, « *la Criminalité électronique* », revue de la législation électronique.

-ELAZZOUZI Ali, « *La confiance numérique au Maroc »,* TIC journal n° 1

- Filiol Eric « *l'ingénierie sociale* ». Linux Magazine n° 42, 2002.

-GHALI.A, « *de la criminalité informatique au Maroc* », Revue Marocaine de Droit des Affaires et des Entreprises n° 17-18, année 2011.

- LEMAN-LANGLOIS Stéphane « Questions au sujet de la cybercriminalité, le crime comme moyen de contrôle du cyberespace commercial » vol. 39, n° 1, 2006.

-OUZGANE Mohammed « *la criminalité informatique a u Maroc* », Revue marocaine d'administration locale et de développement, n°51-52, 2003.

RAPPORTS

-Nouvelles approches de la confiance numérique, Rapport d'expédition Février 2011.
- CISSE Abdoullah, la cybercriminalité en Afrique, 2011.
-Rapport annuel de l'agence nationale de la réglementation des télécommunications (ANRT), 2010.
-Marco Gercke. Comprendre la cybercriminalité: Guide pour les pays en développement, 2009.
-Programme marocain de confiance numérique 2009 ;
-Baromètre annuel sur la cybercriminalité en 2008 par Kaspersky lab.

CODES ET LOIS

-Code pénal marocain
-Droit marocain des obligations et des contrats (DOC)
-Code pénal de l'Etat de Californie
-La loi n°09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel promulguée par le Dahir n° 1-09-15 du 22 safar 1430 (18 février 2009).

-Loi n°53-05 relative à l'change électronique des données juridiques promulguée par le Dahir n° 1-07-129 du 19 kaada 1428 (30 novembre 2007).
-La loi n°07-03 complétant le code pénal en ce qui concerne les infractions relatives aux systèmes de traitement automatisé des données promulguée par le dahir n° 1-03-197 du 11 novembre 2003
-La loi française n°2004-801 du 6 août 2004, qui modifie la loi du 06 janvier 1978 relative à l'informatique, aux fichiers et libertés ;
-La loi française du 5 janvier 1988 dite Loi Godfrain ;
-La loi française n°2000-230 du 13 Mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique.
-la loi n°24-97 relative à la Poste et aux Télécommunication, promulguée par le Dahir n°1-97-162 du 7/08/1997
-la loi n°03-03 relative à la lutte contre le terrorisme Promulguée par le Dahir n° 1-03-140 du 26 Rabiaa 1424 (28 mai 2003)
-la loi n°2-00 relative au droit d'auteur et droits voisins, promulguée par le Dahir n°1-00-20 du 15/02/2000.
-Décret n° 2.11.508 portant création de la Commission Stratégique de la Sécurité des Systèmes d'Information (B.O n° 5988 du 22 Kaada 1432 le 20 octobre 2011)
- Décret n° 2.11.509 portant création d'une Direction Générale de la Sécurité des Systèmes d'Information. (B.O n° 5988 du 22 Kaada 1432 le 20 octobre 2011)

WEBOGRAPHIE

www.justice.gov.ma
www.sgg.gov.ma
www.evasion-e-commerce.blogspot.com
www.01net.com/editorial/514625/comment-hacker-croll-a-pirate-des-comptes-twitter

www.viruslist.com/fr/analysis?pubid=200676286

www.viruslist.com/fr/analysis?pubid=200676168

www.viruslist.com/fr/analysis?pubid=200676286

fr.wikepedia.org/wiki/Script.kiddie

fr.wikipedia.org/wiki/Hacktivisme

www.zone-h.org/mirror/id/4282699

www.mcherifi.org/hacking/cyber-activisme-au-maroc.html

www.arbornetworks.com/report

www.anrt.ma/sites/default/files/rapportannuel/Rapport%20annuel%202010%20_fr.pdf

www.hamza.ma/defacage/docs-justice-gov-ma-portail-documentaire-du-ministere-de-la-justice-pirate

www.bladi.net/des-marocains-impliques-dans-le-piratage-de-cartes-bancaires.html

www.microsoft.com/northafrica/press/Pages/Article.aspx?id=49

http://www.lesoir-echos.com/une-cellule-terroriste-demantelee-a-meknes/presse-maroc