Revue DIAA des Etudes juridique **ISSN 2710-7930**
Année : 2020 **Vol : 01** **No : 01** **Page : 01 - 20**

Cybercriminalité, un fléau planétaire

1. Mlle Nassima AZIZI *
Doctorante en Littératures françaises
Département de Français
Université de Batna 2, Algérie
azizinassima22@yahoo.fr

2. Mlle Ibtissem KHEDRI.
Doctorante en didactique du Français
Département de Français
Université de Batna 2, Algérie
soussoukh1987@gmail.com.

ملخص:
ترتكز دراستنا على إزالة الغموض لأحد أهم الانحرافات في يومنا هذا وهي الجريمة المعلوماتية. هذا المفهوم يندرج أساسا ضمن السياق الاجتماعي–الاقتصادي وحتى السياسي الحالي. في معظم الأحيان ناتج عن سعي المجرم للوصول إلى ضحاياه بل واستمتاعه بتدميرهم ماديا ومعنويا. غايته الأساسية هي الابتزاز بكل أنواعه، لتحقيق أرباح مادية على وجه الخصوص، من خلال خداع الجاني لضحاياه والضحك بشكل ساخر على ظروفهم.
كلمات مفتاحية: الجريمة المعلوماتية –الانحراف –الجاني –الضحية – الابتزاز.

ABSTRACT:
Our study consists of an immanent decoding of one of the most important concepts of our time, and which is constantly evolving, cybercrime. This concept is in essence and par excellence, in the current socio-economic and even political context. It is a drift and delinquency that is an integral part of the cybercriminal's experience. Most often from his desire to enjoy others or even to destroy. Its essential and substantial function is blackmail. It targets the morale as well as the material of the target. It is especially in a space without guard that one deceives and laughs ironically precious victims.
Keywords: Cybercrime - Drift - Offender - Target – Blackmail.

* Correspondant Auteur : Mlle Nassima AZIZI

Introduction :

Dans la société contemporaine, Internet, est devenu au fil des années plus qu'un outil de travail, un véritable support d'éducation, instrument d'acquisition et de vérification des connaissances personnelles, un moyen de communication et plus largement une source d'accès à l'information. En d'autres termes, il constitue une des caractéristiques de la société contemporaine quel que soit le continent considéré. Le développement de l'Internet et sa croissance continue ont un impact significatif sur le développement des sociétés à travers le monde. La société de l'information touche aussi bien les sociétés développés que les celles en développement. Elle est désormais un constituant à part entière et indispensable de leur économie.

Néanmoins, l'essor de la révolution informationnelle de notre époque et dont témoigne notre présent a favorisé l'apparition de nouvelles formes de dérives délictueuses et criminelles, de risques et de techniques de contournement de la loi, qui surgissent automatiquement avec tout développement culturel et technique. Ainsi, la criminalité se développe aujourd'hui sur un terrain moins risqué et plus fertile que celui du monde réel. Ses menaces font courir des risques considérables pour les entreprises, les administrations publiques et les particuliers. la capacité des petits, des grands, des ignorants et des apprenants à l'utiliser sans restrictions ni censure ont conduit à une augmentation de ces dangers et à la propagation des pillages et des vols électroniques; pour préserver les frontières et renforcer la protection, des lois , que le droit doit adoptées pour contraindre les criminels à respecter leurs limites, Ces lois sont appliquées sur le terrain et, en réalité, à cause de l'ignorance de la population car elles constituent des lois nouvelles et modernes pour des crimes peu communs et ne ressemblant pas à d'autres crimes, l'une des étapes les plus importantes de l'application de ces lois consiste à éduquer la population sur la cybercriminalité, son historique, ses caractéristiques, et les principales raisons derrière lesquelles se justifient les cybercriminels .

Définition de la cybercriminalité

La cybercriminalité constitue un acte préjudiciable et tout comportement illégal causés par un individu ou un groupe par le biais de l'utilisation d'appareils électroniques, résultant le gain du cybercriminel d'avantages matériels ou moraux. Cet acte a un effet néfaste sur d'autres personnes et le terme de cybercriminalité porte plusieurs noms, notamment :

— Crimes informatiques et Internet
— Crimes de haute technologie

Malgré les efforts croissants pour lutter contre le phénomène de la criminalité informatique, il n'existe pas de définition spécifique et acceptée par les juristes du concept de criminalité informatique, une partie de la jurisprudence s'est orientée vers la définition étroite du terme et une autre vers des définitions largement connues.

La Commission européenne, définit "cybercriminalité" par trois catégories d'activités criminelles :

- Les formes traditionnelles de criminalité, (fraude et la falsification informatiques = escroqueries, fausses cartes de paiement…)
- La diffusion de contenus illicites par voie électronique (violence sexuelle exercée contre des enfants, incitation à la haine raciale…).
- Les infractions propres aux réseaux électroniques, c'est-à-dire les attaques visant les systèmes d'information, le déni de service et le piratage.

Le juriste Merwe définit la cybercriminalité comme l'acte illicite commis par un ordinateur - ou l'acte criminel utilisé dans la programmation informatique comme un outil majeur. Ros blat la définit par le comme toute activité illégale qui consiste à copier, modifier, supprimer ou accéder aux informations stockées dans l'ordinateur et à en modifier le cheminement. Klaus Tieduman à son tour la définit comme toute forme de comportement illicite commis pour le compte de l'ordinateur.

Le concept de crime informatique est défini comme le crime dans lequel les données informatiques et les programmes d'information jouent un rôle clé.

Le crime informatique comprend l'utilisation des ordinateurs en tant qu'outil pour commettre ce crime, en plus

des affaires d'accès non autorisé à l'ordinateur ou aux données de la victime, y compris les attaques physiques sur les cartes de crédit, la violation des machines de compte automatisées, y compris les chèques. Le transfert de comptes financiers par des moyens électroniques et la falsification des composants physiques et moraux de l'ordinateur, voire le vol de l'ordinateur en lui-même et de l'un de ses composants.

Selon un autre point de vue de la définition de la cybercriminalité, c'est un acte ou un acte d'abstention qui porte atteinte aux composants de l'ordinateur et de ses réseaux de communication, qui sont protégés par le Code pénal et punissables.

Selon la jurisprudence des partisans de cette tendance générale, tout comportement criminel est aidé par l'ordinateur ou par un crime quelconque à proximité d'ordinateurs.

Bien que l'Office of Technology Assessment des États-Unis d'Amérique ait défini le crime d'information comme les crimes pour lesquels les données informatiques et les programmes d'information jouent un rôle majeur, la loi de l'entité sioniste (Israël) relative aux délits informatiques les définit comme des crimes de falsification. Les programmes informatiques gênent leur utilisation, les informations non autorisées ne sont résolues que pour des personnes spécifiques et sont piratées dans le but de commettre un autre crime ou de transmettre un virus qui en altère les performances.

Piliers du phénomène cybercriminel

Les éléments de la cybercriminalité, tels que la criminalité ordinaire, se situent dans les contextes juridique, physique et moral.

1- Le pilier juridique

Dans le cas de la législation algérienne, une section du Code pénal a été introduite dans la section VII bis du chapitre III sur les infractions pénales et les délits mineurs contre l'argent sous le titre de violation des systèmes de traitement automatisé de données.

2 - le pilier physique

L'élément physique de la cybercriminalité comprend le comportement criminel, le résultat et le lien de causalité, bien qu'il soit possible de vérifier l'élément physique sans obtenir le résultat, par exemple en signalant le crime avant que le résultat

ne soit obtenu (par exemple, créer un site pour diffamer une personne sans mettre ce site sur Internet, punit l'acteur.

L'élément physique de ce crime prend plusieurs images en fonction de chaque acte positif commis (par exemple, le crime de fraude d'informations : l'élément matériel consiste à changer la vérité dans les enregistrements électroniques ou les journaux électroniques).

3 - Le pilier moral

Le pilier moral de la cybercriminalité est constitué de deux éléments, à savoir la conscience et la volonté.

- La conscience : est la réalisation des choses réelles.

- La volonté : c'est la direction du comportement criminel d'atteindre le résultat. Selon les principes généraux énoncés dans le Code pénal, l'intention criminelle peut être générale et spécifique, l'intention pénale générale : l'objectif direct de la conduite criminelle et se limite aux limites de l'acte. L'intention pénale privée est ce qui est requis dans certains crimes sans que l'autre ne commette le crime mais s'assure que le résultat est atteint (par exemple, dans le cas du meurtre, l'auteur n'est pas satisfait, mais s'assure plutôt que la victime est tuée).

L'auteur d'un crime électronique dirige sa conduite criminelle vers la commission d'un acte illicite ou non autorisé en ayant la connaissance et l'intention de le faire, et quiconque ne peut nier sa connaissance comme un corps d'intention criminelle générale.

Par conséquent, l'intention criminelle générale est disponible dans tous les crimes électroniques sans exception, mais cela n'empêche pas que certains crimes électroniques ont une intention criminelle particulière (par exemple, infractions de diffamation en ligne et infractions de cybercriminalité).

4. Criminalité électronique

Les auteurs de cybercriminalité sont également appelés pirates informatiques. Ils peuvent être classés en trois catégories :

A. **Pirates informatiques** : Il s'agit de pirates informatiques qui prennent la cybercriminalité, et le piratage informatique est un passe-temps ou une curiosité qui n'existe pas et dont le but est subversif et sans but, La catégorie jeunesse est obsédée par la profondeur de l'information électronique et informatique.

B - **Crackers** : Ce sont des pirates professionnels, et ce type de la plupart des auteurs de cybercriminalité dangereux, et les pirates de cette communauté de statut social ordinaire ou spécialistes en science électronique.

C - **La secte infidèle** : Cette communauté cible souvent des organisations, des entreprises et des employeurs. Le crime contre ces personnes vise généralement à se venger et à obtenir un avantage matériel ou politique, et peut être (des régimes extrêmes, espions ou pénétrants).

Les motivations de la cybercriminalité peuvent être motivées par des motivations matérielles afin de satisfaire le désir de richesse ou de motivation personnelle, d'apprentissage, d'apprentissage, de vengeance et de divertissement politique.

Pour que les pirates informatiques puissent mener à bien leur cybercriminalité, plusieurs outils sont nécessaires.

Outils et auteurs de cybercriminalité

Les pirates peuvent mettre en œuvre leur crime en ligne en fournissant des outils à savoir :

- L'accès à Internet est un outil essentiel pour l'exécution du crime.
- Un logiciel spécial pour copier les informations stockées par l'utilisateur sur ordinateur.
- Dispositifs d'espionnage, y compris connexion d'appareils photo avec des lignes téléphoniques.
- Le code à barres est un outil utilisé pour numériser le codage numérique et décoder le code.
- Imprimantes.
- Téléphones numériques et mobiles.
- Des programmes malveillants, dont le cheval de Troie qui a pour fonction de tromper la victime.

Objectifs d'une criminalité réelle dans un monde virtuel

En matière de cybercriminalité, nous pouvons résumer en quelques points certains des objectifs de la cybercriminalité, notamment :

- L'accès à des informations de manière illégale, tel que voler des informations, les visualiser, les supprimer ou les modifier pour atteindre l'objectif du délinquant.
- Accès aux serveurs d'information par l'intermédiaire du Web.

- Obtenir et faire chanter des informations confidentielles sur des utilisateurs de technologies tels que des institutions, des banques, des agences gouvernementales et des particuliers.
- Les gains matériels, moraux ou politiques illégaux générés par les technologies de l'information, tels que le piratage et la destruction de sites Web, la contrefaçon de cartes de crédit, le vol de comptes bancaires, etc.

Origine et évolution de la perception de la menace cybercriminelle

Le premier cas de cybercriminalité a eu lieu avant même l'apparition d'Internet, on a conçu internet et les réseaux informatiques pour créer, stoker et transférer des informations gouvernementales. La création de ces méthodes numérisées a aidé l'humanité à se développer au 21ème siècle, mais elle a également aidé les criminels. Ces derniers qui veulent accéder à l'information, et compliquer, à la suite, son exploitation juste pour prouver qu'ils sont capables d'y avoir accès.

Comment la cybercriminalité a-t-elle évolué ?

Les premiers crimes de ce genre étaient des cas de hacking simples pour capter des informations à travers des réseaux locaux, mais avec l'ampleur qu'a pris internet, la cybercriminalité s'est aussi développée.

La première grande vague de cybercriminalité est apparue à la fin des années 1980, une série d'escroqueries a livré à une boîte de réception. : « Salutations, je suis un prince descendant du Nigeria. J'ai besoin d'aide pour sortir des millions de mon pays, tout ce que vous avez à faire est de m'envoyer un peu d'argent pour configurer le transfert. Une fois terminé, je partagerai mes millions avec vous » … oui, c'est cela.

La prochaine vague dans l'histoire de la cybercriminalité est effectuée dans les années 90 avec le développement des navigateurs Web, à l'époque, on avait plusieurs choix, bien plus qu'aujourd'hui puisque la plupart des navigateurs étaient vulnérables aux virus. Les virus étaient livrés à partir des connexions Internet après la consultation de sites Web douteux. Il y a des virus qui ont provoqué le ralentissement de l'ordinateur, d'autres causent l'apparition de publicités et polluaient l'écran et redirigent vers des sites pornographiques.

La cybercriminalité s'est vraiment propagée au début des années 2000 avec l'apparition des réseaux sociaux. Les gens mettent en place des bases de données avec toutes les données du profil, ce qui a engendré une inondation d'informations personnelles et par conséquent le vol d'identité. Les voleurs utilisent l'information pour accéder aux comptes bancaires, faire des demandes de cartes de crédit ou effectuer des fraudes financières.

La dernière vague consiste à créer une industrie criminelle mondiale qui compte totalisant un demi-milliard de dollars par an. Ces criminels utilisent des méthodes minutieuses grâce à leur présence sur le web.

Quelques dates clé de la cybercriminalité

Il est impossible d'identifier la première date dans laquelle on a commis un méfait sur le réseau informatique, mais, on peut préciser la première attaque majeure sur un réseau informatique pour la considérer plus tard comme un point de référence concernant l'évolution de la cybercriminalité.

1971 – John Draper, un « phone freak », découvre qu'un sifflet offert en cadeau dans des boîtes de céréales Cap'n Crunch produit les mêmes sonorités qu'un téléphone qui gère des ordinateurs. Phone phreak est un terme utilisé pour décrire les programmateurs informatiques fascinés par les réseaux téléphoniques. Il a construit une « boîte bleue » avec le sifflet qui lui a permis d'émettre des appels téléphoniques interurbains gratuits, puis a diffusé des instructions pour expliquer comment le faire.

1973 – Un caissier d'une banque de New York a utilisé un ordinateur pour voler plus de 2 millions de dollars.

1978 – on a diffusé en ligne le premier système de communication global et cela est rapidement devenu une méthode de communication très répandue dans le cybermonde. Elle a permis l'échange rapide et gratuit de connaissances, grâce aux astuces de piratage.

1981 – le capitaine Zap est la première personne reconnue coupable d'un acte de cybercriminalité. Il a piraté le réseau AT & T et a changé l'horloge interne pour ajouter des heures supplémentaires aux heures de pointe et a été une source d'inspiration pour le film *Sneakers*.

1983 – Le film *War Games* sort et informe le public sur le piratage électronique. Le film parle d'un adolescent qui

pénètre le système informatique du gouvernement à travers une porte arrière et mène le monde vers la troisième guerre mondiale.

1986 – Le Congrès a choisi le Computer Fraud and Abuse Act, qui rend illégal le piratage et le vol.

1990 – La Legion Of Doom et les Masters Of Deception, deux cybergangs, se sont engagés dans la guerre en ligne. Ils ont bloqué activement les connexions les uns des autres, piratent les ordinateurs et volent les données.

1993 – Kevin Poulson est condamné pour avoir piraté des systèmes téléphoniques. Il a pris le contrôle de toutes les lignes téléphoniques dans une station de radio à Los Angeles pour gagner à jeu sur appel téléphone, il s'est enfoui mais on l'a piégé plus tard. Il a été condamné à 5 ans de pénitencier fédéral et a été le premier à se voir interdire l'utilisation d'Internet pendant sa peine.

1999– l'apparition du virus Melissa. Il devient l'infection informatique la plus virulente et conduit à l'une des premières condamnations pour quelqu'un ayant rédigé des logiciels malveillants. Le virus Melissa était un macrovirus qui cible les comptes de messagerie pour les faire effectuer des envois de masse. L'auteur du virus a été accusé d'avoir causé plus de 80 millions de dollars de dommages aux réseaux informatiques et a été condamné à 5 ans de prison.

2002 – Le site Web de Shadow Crew est lancé. C'est un site d'échange et un forum pour les cyber-pirates. Les membres peuvent publier, partager et apprendre à commettre divers cas de cybercriminalité et éviter de se faire prendre. Le site a duré deux ans avant d'être fermé par le service secret.

2003 – SQL Slammer devient le virus qui se propage le plus rapidement dans l'histoire. Il infecte les serveurs SQL et engendre une attaque par déni de service qui affecte les vitesses sur Internet pendant un certain temps.

2007 – l'augmentation des cas de piratage, de vol de données et d'infections par des logiciels malveillants. Le nombre de documents volés, de machines infectées a multiplié, ainsi que le montant des dommages causés. On a accusé le gouvernement chinois d'avoir piraté les États-Unis et d'autres systèmes gouvernementaux.

Aujourd'hui, la cybercriminalité a fortement augmenté, en effet, elle est l'une des formes de délinquance qui connaît

l'augmentation la plus forte. Le nombre de malfaiteurs en ligne ne cesse de croître… Cela s'explique par la très forte évolution du nombre d'internautes. Ce phénomène d'extension d'Internet, l'évolution du nombre d'internautes et la mondialisation permet aux individus malveillants, les « cyber-délinquants » qui rodent sur la toiles, d'innover dans les crimes sur Internet et de se livrer à presque n'importes quelles activités illicites sur le plan International.

Caractéristiques des infractions informatiques

Les crimes commis par ordinateur en tant qu'outil ou en tant que cible d'un crime se caractérisent par les caractéristiques suivantes :

- **Rapidité d'exécution :** l'exécution du crime par téléphone ne nécessite pas beaucoup de temps et, en un clic, des millions de dollars peuvent être transférés d'un lieu à un autre. Cela ne signifie pas qu'ils ne nécessitent pas d'installation avant la mise en œuvre ou l'utilisation de matériel et de logiciels spécifiques.
- **Exécution à distance:** dans la plupart des cas, les crimes informatiques (sauf le vol de matériel informatique) n'exigent pas la présence de l'auteur sur le lieu du crime, mais l'acteur peut commettre son crime dans un pays éloigné de l'acteur, que ce soit en entrant dans le réseau concerné ou en faisant objection à un transfert financier, ou vol d'informations importantes ou sabotage ... etc.
- **Masquer le crime :** Les crimes qui se produisent sur l'ordinateur ou par le biais de celui-ci en tant que crimes (Internet) sont des crimes cachés, mais vous pouvez en remarquer les effets et les deviner.
- **Gravité:** le marché de l'informatique et de l'Internet représentant une grande richesse de criminels ou d'objets organisés, il est devenu plus intéressant d'investir et de blanchir de l'argent, dont beaucoup sont utilisés pour développer des techniques et des méthodes permettant d'accéder à des réseaux, de voler des informations et de les vendre, de voler des banques, d'intercepter des transactions financières, numéros de carte ... etc.
- **Phénomène international :** La connexion du monde à un réseau de communications par satellite, et par Internet a rendu possible la diffusion culturelle et la mondialisation de

la culture et de la criminalité, sans reconnaître les frontières territoriales des pays, des lieux, des époques et du monde. Dans la société de l'information, les frontières géographiques séparent les États car le monde est connecté à un réseau unique, où la plupart des crimes commis sur Internet sont le contrevenant dans un État et la victime dans un autre État, et les dommages causés par le crime peuvent ne pas être ceux de la victime sur le territoire de l'auteur. Et les matériaux présentés sont incompatibles avec les cultures destinataires, en particulier s'ils sont en conflit avec la religion, les coutumes, l'ordre social et moral et l'ordre politique de l'État.

- **Crimes :** Les crimes classiques exigent le recours à des outils et à la violence, tels que des crimes de terrorisme et de drogue, vol et vol à main armée. Les crimes liés à l'informatique sont toutefois qualifiés de crimes non violents ne requérant pas la violence. Le transfert de données d'un ordinateur à un autre ou le vol électronique de soldes bancaires ne toute violence ou échange de feu avec le personnel de sécurité.
- **La difficulté de le prouver :** la criminalité sur Internet est caractérisée par la criminalité traditionnelle comme difficile à prouver, en raison de l'absence des effets traditionnels de la criminalité, de l'absence de preuves matérielles (empreintes digitales, dévastation, preuves matérielles) et de la facilité d'effacement ou de destruction des preuves en très peu de temps. En plus, la police et le système de justice, et les lois existantes sont souvent inadéquates.
- **Pollution culturelle :** L'impact de la criminalité liée à l'informatique ne dépend pas de son impact physique, mais plutôt du système de valeurs et du système moral, en particulier dans les sociétés conservatrices et fermées.
- **Criminalité mondiale et système judiciaire :** Compte tenu de la connexion électronique de la communauté internationale, notre société est devenue une fiction, ce qui a permis à la communauté internationale de trouver sa place dans tous les pays et dans toutes les sociétés du monde en tant que lieu de crime. Nouvelle législation visant à lutter contre la criminalité informatique, exigeant que les lois soient universelles.

- **La cybercriminalité n'est pas souvent signalée** : du fait que la victime n'a pas été identifiée ou a peur de la diffamation il ne déclare pas ce genre de crime. La quasi-totalité de la cybercriminalité a donc été découverte par hasard et, même après une longue période de perpétration, les crimes non découverts sont bien plus que ceux qui ont été révélés. Le chiffre sombre entre le nombre de crimes commis et le nombre découvert est un nombre grave. L'écart entre le nombre de ces crimes réels et ce qui a été découvert : un grand écart.
- En théorie, il est facile de commettre un crime de nature technique, mais aussi de cacher les caractéristiques du crime et la difficulté de suivre les auteurs.
- Par conséquent, ces crimes n'ont plus d'effet une fois qu'ils ont été commis, outre la difficulté de conserver les effets artistiques éventuels. Il n'ya pas d'argent ni de bijoux, mais les chiffres changent, ce qui fait que la plupart des actes de cybercriminalité ont été découverts par hasard et longtemps après qu'ils ont été commis.
- Ces crimes reposent sur le plus haut niveau d'intelligence et il est difficile pour l'interrogateur traditionnel de traiter ces crimes. Il lui est difficile de suivre les crimes commis sur Internet, de les découvrir et de les prouver. Il s'agit d'infractions ambiguës ; il est différent de les prouver et de les enquêter que d'enquêter sur des crimes traditionnels.
- L'accès à la vérité nécessite le recours à une expertise technique de haut niveau.
- La mondialisation de ces crimes entraîne la dispersion des efforts internationaux en matière d'enquêtes et de coordination visant à assurer le suivi de ces crimes ; ces crimes donnent une image fidèle de la mondialisation ; en termes de lieu, ces crimes peuvent être commis à distance et cet endroit peut représenter plus d'un pays ; Ce qui soulève la question de : Déterminer le droit applicable à ce crime.
- La difficulté de réclamer des dommages-intérêts civils pour cybercriminalité.

Certaines méthodes, les plus importantes, de cybercriminalité sont les suivantes :

- La fabrication et la diffusion de virus, l'un des crimes les plus courants et les plus répandus sur Internet

- Arrêtez des services en les déversant avec un grand nombre de demandes, ce qui entraîne la chute du serveur et arrêter le travail immédiatement.
- Usurpation d'identité.
- Diffuser la réputation en publiant des informations obtenues illégalement par le contrevenant et en affirmant que ces actes ont un but matériel, politique ou social.
- Fraude, telle que la vente de biens ou de services virtuels.

Les méthodes les plus importantes de prévention du piratage et de la cybercriminalité sont les suivantes :

- Prenez garde et ne pas croire toutes les annonces et s'assurez de leur crédibilité.
- Évitez d'ouvrir un courrier électronique anonyme et même de l'annuler tout de suite.
- Mettez le code secret en conformité avec les bonnes spécifications qui rendent difficile le piratage : il doit contenir plus de huit caractères, être composé de lettres, symboles, langues, etc.
- Prendre soin des informations personnelles et de son ordinateur en développant des programmes de protection appropriés

Causes de la criminalité électronique

Les causes de la cybercriminalité sont multiples, elles varient en fonction, du type de cible, et du niveau d'exécution (individuel, sociétal, économique). Les crimes des jeunes amateurs diffèrent des crimes commises par les professionnels et varient en fonction du but recherché : vol, informations commerciales, informations personnelles, etc.

Les causes de la criminalité au niveau individuel

1- Recherche de reconnaissance (souci de reconnaissance)

Les jeunes téméraires commettent des actes de cybercriminalité pour contester et être reconnu dans les médias. Cette catégorie arrête souvent ce comportement à un âge plus avancé après les vingt ans.

2- Opportunité

Les technologies modernes et Internet offrent des possibilités sans précédent de propagation de la cybercriminalité. L'éducation joue un rôle majeur dans la production de crimes et la violation des normes sociales. L'absence de censure augmente les risques de cybercriminalité.

Et ainsi, la probabilité de détection de l'acteur est faible. Les TIC et l'utilisation croissante d'Internet ont créé de nouvelles opportunités pour les criminels et facilité la croissance de la cybercriminalité, qui est une forme de criminalité nouvelle et distincte.

3- Faible maîtrise de soi

On s'appuie sur la théorie générale du comportement téméraire, qui affirme que la possibilité que des individus se livrent à un acte criminel résulte de la possibilité d'une faible maîtrise de soi, ce qui indique la nature du comportement irresponsable à partir des caractéristiques des personnes, le comportement inconsidéré est une manifestation de faible maîtrise de soi et, comme dans la théorie du contrôle social de Hershey, les motivations pour la conduite de comportements irresponsables ne changent pas car chaque individu peut se précipiter pour atteindre ses intérêts personnels, y compris le comportement téméraire. Un comportement non intentionnel est une tâche facile et peut rapidement concrétiser des intérêts particuliers, tels que la corruption, le vol et d'autres actes criminels, rapidement et facilement, sans attente ni effort. Mais la différence entre les individus réside dans le degré de maîtrise de soi et dans la possibilité de commettre un comportement déviant.

La faible maîtrise de soi et la possibilité d'adopter un comportement irresponsable sont des facteurs déterminants dans la conduite d'un comportement imprudent. Gerdstone et Hershey ont tenté d'attribuer les différences entre les criminels à des différences de contrôle de soi. Le moi est une force naturelle qui apparaît en l'absence d'étapes pour son développement, c'est-à-dire le produit d'une socialisation incomplète, où les parents ne surveillent pas leur enfant et ne remarquent pas un comportement déviant.

Au contraire, la maîtrise de soi peut affecter les performances des personnes dans des institutions telles que l'école, le travail, le mariage et les personnes à faible estime de soi non seulement tendant aux comportements déviants, mais échouant souvent à l'école, au travail ou au mariage.

Des études ont également montré qu'une faible maîtrise de soi et une faible tolérance au risque pour des gains à court terme pouvaient s'appliquer aux actions pouvant être facilitées ou améliorées par Internet. De plus, les individus en ligne sont

exposés à des modèles d'apprentissage criminels et leurs pairs sont plus susceptibles de se livrer à la criminalité. La théorie de l'apprentissage social peut avoir une application particulière en ce qui concerne les cybercriminels : les criminels doivent souvent apprendre des techniques. La théorie générale du crime et la théorie de l'apprentissage social montrent que les individus se comportent de manière respectueuse dans l'environnement virtuel comme ils agissent dans le monde réel.

4- Activité de routine

L'augmentation du nombre de victimes de la cybercriminalité peut s'expliquer par les changements introduits dans la vie quotidienne des individus : avec l'avènement d'Internet, la façon dont les gens communiquent ou interagissent avec les autres dans le cadre de relations personnelles, de divertissements, de commerce, etc.

Les changements dans les activités de routine des utilisateurs, tels que l'utilisation du Net et les réseaux sociaux tels que Facebook, la messagerie électronique, les sites Web, etc., ont créé des opportunités pour les criminels avec des cibles faciles et précieuses dans l'espace sans garde.

Cohen et Wilson suggèrent que le crime est susceptible de se produire en présence de trois facteurs - le coupable motivé, la cible appropriée et l'absence de tuteurs.

Les causes de la criminalité au niveau communautaire

1- L'urbanisation

L'urbanisation est l'une des causes de la cybercriminalité en général, caractérisée par de fortes migrations des campagnes vers les villes, les agglomérations urbaines et les grandes villes. Les jeunes qui ne sont pas en mesure de faire face à la demande de la vie urbaine, ce qui les oblige à vivre dans des bidonvilles et des quartiers périphériques et marginalisés, et à faire face à la concurrence, ces derniers sont incapables de suivre le rythme c'est pourquoi ils choisissent la cybercriminalité, pour laquelle ils n'ont pas besoin de gros capitaux.

Selon Mick, l'urbanisation est une cause majeure de la cybercriminalité au Nigeria et l'urbanisation sans criminalité est impossible, ce qui a permis aux élites de constater que l'investissement dans la cybercriminalité est rentable.

2- Le chômage

Comme le crime traditionnel, la cybercriminalité est liée au chômage et aux conditions économiques difficiles. Le nigérian dit : "L'esprit des chômeurs est un atelier pour le diable." Ainsi, les jeunes connaisseurs investiront dans la cybercriminalité.

3- Pressions générales (souches)

Les pressions générales exercées sur la société sont la pauvreté, le chômage, l'analphabétisme, des conditions économiques difficiles et des facteurs de stress pour la société en général et pour le secteur de la jeunesse en particulier, ce qui génère des sentiments négatifs chez une grande partie de la population face aux circonstances et à la société, ainsi, on adopte des comportements négatifs.

4- La recherche de la richesse (Quête de la richesse)

La théorie générale du crime de Gefredsson et de Hershey soutient que les gens cherchent des moyens socialement inacceptables d'atteindre des objectifs socialement acceptables. La cible est plus grande, plus facile à mettre en œuvre, plus rapide et moins risquée.

De nombreux pays n'ont pas mis au point de législation ni de système judiciaire pour pouvoir suivre l'évolution de la cybercriminalité et de ses méthodes, ce qui ne dépend pas de la législation, mais en rapport avec la police, les enquêtes, le système judiciaire et la manière de traiter les preuves numériques au niveau national et international. En effet, les techniques disponibles sont souvent très modestes, de même que des experts en mesure de surveiller et poursuivre les auteurs de cybercriminalité.

Les causes de la criminalité au niveau mondial

1- Transformation de la société numérique

La société numérique actuelle est caractérisée par trois caractéristiques principales :

- Les changements quantitatifs dans le type d'informations qui circulent, en raison de la technologie des communications et des transports, des images et des informations couvrant le monde rapidement et avec précision.
- Envoi d'informations à de nombreuses parties (personnes et équipements) : ces informations dirigent le

missile et envoie le rapport et la diffusion en direct à partir du lieu de la manifestation.

— La présence de réseaux d'échange d'informations entre toutes les parties, tels que le courrier électronique, mobile, etc.

Nous sommes entrés dans l'ère des nouvelles technologies de l'information (cyberespace ou monde virtuel) : les gens passent une partie de leur vie quotidienne dans le cyberespace, créant des réseaux et des sites, profitant de nouveaux types de relations sociales et communiquant avec ce qui se passe dans le monde extérieur. Tout le monde peut avoir un ordinateur ou un modem avec peu de connaissances techniques, autrement dit, Internet a créé ce que l'on appelle maintenant le cyberespace ou le monde virtuel. La société doit assumer ses fonctions jusqu'à ce que la sécurité soit atteinte.

2- La mondialisation

L'émergence du cyberespace crée de nouveaux phénomènes distincts de l'existence des systèmes informatiques eux-mêmes et des opportunités criminelles immédiates offertes par les ordinateurs dans le cyberespace : les individus peuvent présenter des différences quant à leur propre conformité (légale). Par exemple, ils peuvent commettre des crimes dans le cyberespace qu'ils ne commettent pas dans le monde réel en raison de leur statut. De plus, la souplesse de l'identité, le manque d'identité stimulent le comportement criminel dans le monde virtuel.

3- Interdépendance mondiale

L'émergence d'une interdépendance mondiale dans le contexte des transformations économiques et démographiques du monde est un facteur susceptible de contribuer à la progression de la criminalité. D'ici 2050, la population urbaine doublera pour atteindre 6,2 milliards, soit 8,9 milliards d'habitants attendus à 70% de la population mondiale. Un rapport du Centre National de la Criminalité en col blanc confirme que l'espace Internet offre aux criminels de nouvelles possibilités de communication avec les victimes, il a été démontré que les caractéristiques uniques d'Internet sont l'anonymat de la personne et que la facilité d'utilisation a fourni aux criminels de nouvelles manières de commettre leurs crimes,

en plus Internet a permis de communiquer rapidement et en toute sécurité avec des criminels.

Conclusion

Le progrès technique a facilité notre mode de vie, mais il a également apporté beaucoup de dangers liés à l'ordinateur et à Internet, ce qui a incité les gouvernements et les responsables à la nécessité de sensibiliser à ces crimes en luttant contre ce fléau planétaire. La lutte contre la cybercriminalité est devenue donc un défi majeur mondial en raison de la dimension internationale de cette nouvelle délinquance souvent organisée. Une volonté réglementaire existe bien au niveau international de pouvoir maîtriser la cybercriminalité. En effet, il faudrait sensibiliser les gouvernements et les sociétés à la nécessité d'éveiller la conscience du public et de dénoncer ces crimes en les expliquant à la population. Aussi, on devrait exhorter les universités et les centres de recherche à étudier la cybercriminalité et à créer des diplômes spécialisés dans les domaines techniques et juridique liés à la lutte contre ces crimes. De plus, on doit former de cadres humains travaillant dans ce domaine de la lutte contre la criminalité informatique. Cette époque nécessite des institutions de sécurité conçues pour faire face aux mutations rapides, en mettant l'accent sur l'innovation, la transparence et la satisfaction du client (l'ensemble de la communauté), des institutions rapides pour la diffusion d'informations et l'information du public. Des institutions capables de se redéfinir pour faire face à la cybercriminalité rapide et en mutation rapide.

Pour finir, la difficulté et la complexité du chantier à mettre en œuvre et les moyens nécessaires pour atteindre les objectifs de lutte contre non seulement la cybercriminalité mais aussi le crime organisé, met la société mondiale devant un nouveau défit plus sophistiqué, qui fait que l'Internet est exploité à des fins malveillantes.

Bibliographie

Ouvrages consultés

FILIOL, Eric. Cybercriminalité : Les Mafias Envahissent le Web. Paris : Dunod, 2006. 224 p. (Coll. QUAI DES SCIENC). ISBN-13: 978-2100502783

FREYSSINET, Éric. La Cybercriminalité en Mouvement. Paris : Hermes Science Publications, 2012. 240 p. (Coll. Management et informatique). ISBN-13: 978-2746232884

GHERNAOUTI-HELIE, Solange. La Cybercriminalité : Le visible et l'invisible. Paris : PPUR, 2009. 124 p. (Coll. Le savoir suisse). ISBN-13: 978-2880748487

GUEYE, Papa. Criminalité Organisée, Terrorisme et Cybercriminalité : Réponses de Politiques Criminelles. Sénégal : Harmattan, 2018. 436 p. ISBN : 978-2-343-14769-7

QUEMENER, Myriam. Cybercriminalité - droit pénal appliqué. Paris : Economica, 2010. 272 p. (Coll. Pratique du droit). ISBN-13: 978-2717859027

STAMBOLIYSKA, Rayna. La Face Cachée d'Internet : Hackers, Dark Net...Paris : Larousse, 2017. 352 p. (Coll. Hors collection Société). ISBN-13: 978-2035936417

TOURÉ, Papa Assane. Le Traitement de la Cybercriminalité devant le Juge : L'exemple du Sénégal. Paris : L'Harmattan, 2014. 618 p. ISBN : 978-2-336-30473-1

VENTRE, Daniel. Cyberattaque et Cyberdéfense. Paris : Hermes Science Publications, 2011. 312 p. (Coll. Cyberconflits et cybercriminalité). ISBN-13: 978-2746232044

Sites consultés

BOOS, Romain, 2016. La lutte contre la cybercriminalité au regard de l'action des États. Droit. Université de Lorraine, Français. Disponible via l'URL < https://tel.archives-ouvertes.fr/tel-01470150/document.(Consulté le 12.02.2019)

Cybercriminalité : menaces réelles et mesures quasi-inexistantes, [en ligne]. (Consulté le 09.02.2019) Disponible via l'URL : http://www.anti-cybercriminalite.fr/article/cybercriminalit%C3%A9-menaces-r%C3%A9elles-et-mesures-quasi-inexistantes

Dossiers Sécurité : La cybercriminalité [en ligne]. (Consulté le 08.02.2019) Disponible via l'URL : http://www.wikayanet.dz/index.php/fr/dossiers-securite/1175-la-cybercriminalite?fbclid=IwAR2455yL9UIqQAR7Jrj7QChp53NqsELsCN6V8QoMs9krq-tC9cYYRqLqHg8

GUEHAM, Farid. La délinquance de l'avenir : la cybercriminalité[en ligne]. (Consulté le 11.02.2019) Disponible via l'URL : http://www.trop-libre.fr/la-d%C3%A9linquance-de-l%E2%80%99avenir%C2%A0-la-cybercriminalit%C3%A9-

%C2%A0/?fbclid=IwAR0RNBdG7k6zb1kv4AZvyP0OSobEk0zqvzeNWVmzREb4ForEvRX-BfmYzlI

La cybercriminalité, un phénomène incontrôlable ? [en ligne]. (Consulté le 10.02.2019) Disponible via l'URL : https://lacybertpe.blogspot.com/p/i-les-liens.html?m=1&fbclid=IwAR3w4F0TL0CLVJJnTP6wcONA5QCXaLunhTa2oxbUTbqAun6Aio7zvsHDQr0

ROSE, Coline. Chercheur dans le domaine de la piraterie sur Internet. Discours prononcé lors de l'ouverture du G-8 sur la cybercriminalité. Paris, 2000. [en ligne]. (Consulté le 10.02.2019) Disponible via l'URL : https://tel.archives-ouvertes.fr/tel-01470150/document

MELANI, 10 ans d'histoire de la cybercriminalité, [en ligne]. (Consulté le 12.02.2019) Disponible via l'URL : https://www.ledecodeur.ch/2015/05/06/10-ans-dhistoire-de-la-cybercriminalite-avec-melani/amp/?fbclid=IwAR2IRbf1R8SjZYw0EamRwopx8Ydp-UaSCQGQisR