Communication

CRIMINALITÉ INFORMATIQUE, MENACE DE LA VIE SOCIALE.

CHIZA BYAMUNGU Delphin*

Résumé

Cet article détaille les œuvres de la délinquance informatique. Il met en place un aperçu général sur la criminalité informatique. L'article dresse un panorama de la criminalité informatique, analyse les comportements les outils utilisés par des malfaiteurs, et expose les moyens techniques pour la protection et la prévention contre cette criminalité informatique.

Mots-clés : Criminalité informatique, virus informatique, délinquance informatique.

COMPUTER CRIME, THREAT TO SOCIAL LIFE

Abstract

This article details works of computer delinquency, a general overview on computer crime. The author addresses a set of computer crimes, analyses behaviors and tools used by hackers, and presents technical means to secure and prevent against computer hacking (computer crime).

Keywords: Computer hacking, computer virus, computer delinquency.

INTRODUCTION

La criminalité informatique est un phénomène à la une à l'ère actuelle. Ainsi, il se remarque une montée de la délinquance informatique engendrée par le développement rapide des nouvelles technologies de l'information et de la communication inquiétant de plus en plus les pays, les organisations, les services de police et les particuliers concernés. Au cours de ces dernières années, cette criminalité qui menace la sécurité de la société de l'information a été prise très au sérieux par les humains de tous les pays de l'Afrique voire du monde.

La criminalité informatique ne recouvre pas une catégorie d'infractions clairement définie, mais un ensemble flou d'activités illicites liées à l'informatique. Elle

* Ingénieur Informaticien, Assistant2 à l'Institut Supérieur Pédagogique de Matanda/Masisi Nord-Kivu, Département de Sciences Commerciales et Administrative. Secrétaire Général Académique de l'Institut Supérieur des Techniques et Travaux du Congo à Goma. Tél :(+243) 993772278, 898500991 ; E-mail : yadelphino@gmail.com

est un vaste domaine, dont les frontières ne sont pas toujours faciles à définir. Chaque pays a une législation différente à ce sujet. La plupart des spécialistes ont tendance à proposer une classification qui distingue les affaires où l'ordinateur et le réseau informatique sont la cible de celles dans laquelle l'ordinateur ou le réseau informatique sont les instruments.

La problématique de notre travail, consiste à examiner le fléau dit criminalité informatique, les moyens par lesquels cette pratique mafieuse s'applique et ses conséquences sur la vie humaine. Autrement dit, il s'agit d'étudier cette menace sociale longtemps oubliée et de mettre à nu les outils utilisés par des malfaiteurs et présenter les moyens techniques pour la protection et la prévention contre cette criminalité informatique.

Le système de codification des infractions informatiques recense plus de trente types d'infractions[1]. Parmi tous ces types d'infractions informatiques nous citons : les cas des intrusions informatiques, des piratages téléphoniques, des virus informatiques, drone assisté par l'informatique et de la pédophilie sur Internet qui sont la criminalité informatique la plus fréquente[2]. Pour mieux se protéger des pirates, mieux vaut bien les connaître. Donc il est indispensable de savoir les motivations, les techniques, les comportements et les moyens des criminels informatiques pour établir les mesures techniques et juridiques de protection et de prévention susceptibles de réduire les risques. La prévention et la lutte contre la criminalité informatique pose une série de problèmes techniques, juridiques et de coopération internationale. Mais cela ne concerne pas seulement la police judiciaire ; la prise sociale de conscience de l'importance de la sécurité informatique à tous les niveaux de la société est extrêmement importante.

Pour mener à bien cette recherche, nous nous sommes servis de deux méthodes, la Méthode descriptive et la Méthode analytique: Méthode descriptive consiste à décrire, nommer ou caractériser un phénomène, une situation ou un évènement de sorte qu'il apparaisse familier[3]. Cette méthode nous aide dans la description du sujet du travail pour mieux appréhender les différentes réalités qui s'y trouvent. Tandis que la Méthode analytique consiste à décomposer l'objet d'étude en allant du plus complexe au plus simple. Cette méthode nous permet de synthétiser les données, les informations obtenues et de lister les techniques, les comportements et les moyens utilisés par des criminels informatiques ; enfin la prévention contre cette criminalité.

---

[1] https://www.enssib.fr*Criminalité Informatique*. Consulté le 1ère Juillet 2022 à 13h00
[2] https://www.enssib.fr*Criminalité Informatique*. Idem
[3] N'DA P., *Méthodologie de la recherche, de la problématique à la discussion des résultats,* Éditions Universitaires de Côte d'Ivoire, Abidjan, 2002, P.19

I. DESCRIPTION DE LA CRIMINALITE INFORMATIQUE

I.1. La genèse de la criminalité informatique

L'ordinateur ne date pas d'aujourd'hui. Il a déjà permis aux Américains, il y a quelque cinquantaine d'année, d'obtenir la maitrise de l'atome et de mettre fin à la Seconde Guerre mondiale. Vingt-cinq ans plus tard (16 juillet 1969), les gigantesques «computers» de la NASA (National Aeronautics and Space Administration) leur frayaient la voie de l'espace, pour envoyer le premier homme sur la lune[4]. Mais, il s'agissait alors d'installations d'une dimension, d'un coût et d'une complexité telles que seuls des États ou, à la rigueur, de grandes compagnies pouvaient se les procurer et les utiliser, en faisant appel à des techniciens de haut niveau. Autant dire qu'à l'époque, ce qu'on appellera plus tard l'informatique, était une affaire de spécialistes de haut vol, et totalement inaccessible au commun des mortels.

La situation actuelle est radicalement différente. Au cours de la quatrième génération des ordinateurs en 1980[5], la miniaturisation des ordinateurs, la simplification extrême de leurs procédures d'utilisation, l'abaissement considérable de leur prix, ont fait qu'ils sont devenus un outil de la vie courante et qu'ils régissent de plus en plus tous les domaines de l'activité humaine. Ainsi, les ordinateurs, les systèmes d'information et Internet occupent une place prépondérante dans notre vie. Notre société est de plus en plus dépendante de l'information. Où que nous soyons, quoi que nous fassions, nous risquons d'avoir affaire, directement ou indirectement à un ordinateur, ou un système d'information. Lorsque nous payons avec notre carte de crédit, réservons une place dans un avion, plaçons de l'argent sur notre compte en banque et même lorsque nous passons un simple coup de téléphone, c'est toujours un ordinateur ou un système qui s'occupe de nous. Le développement des technologies de l'information et de la communication a bouleversé tous les secteurs de la société et la naissance d'une société informatique influencera tous les aspects de la vie quotidienne. Les criminels savent aussi tirer parti de la technologie informatique pour commettre des crimes et porter préjudice aux utilisateurs peu méfiants. En 1983, seuls 200 ordinateurs étaient connectés à l'internet. Aujourd'hui, des millions d'ordinateurs sont désormais reliés entre eux dans le monde entier par l'intermédiaire de différents systèmes de télécommunication dont le plus connu est Internet[6]. L'idée de base d'internet est venue des militaires américains qui en 1968 ont voulu avoir à leur disposition un système de connexion qui résiste à toutes les attaques y compris nucléaires. Si une voie est coupée dans la communication, les paquets d'informations munis chacun d'une adresse finale et d'un code permettant de les

[4] https://www.universalis.fr « Encyclopédie universalis » consulté le 1 juillet 2022 à 13h00
[5] https://www. CoursTechInfo.be « *Historique – Les générations d'ordinateurs de 1945 à nos Jours* »
[6] II s'agit de 40 à 80 millions d'utilisateurs sur Internet, selon M. Duncan, *lutte contre la criminalité sur l'inforoute*, la Gazette de la GRC, vol59, n°10, 1997.

ordonner s'orientent vers un autre chemin pour parvenir à destination. Grâce à ce réseau, l'utilisateur peut entrer en communication avec un réseau situé en presque n'importe quel point du globe. Si l'utilisateur dispose du mot de passe ou du code d'autorisation voulu, il peut ainsi accéder à tous les fichiers du système. Il est généralement admis que la capacité du Réseau Internet à stocker et à diffuser d'énormes quantités de données, c'est un bienfait pour la société, mais que sa capacité à favoriser la prolifération d'activités illégales constitue aussi un danger dans la société. II en va de même pour les criminels qui sont, eux aussi, capables d'en tirer profit. Pour ce faire, il ne faut pas négliger les aspects systèmes et réseaux. Avec un certain niveau d'expertise, il est techniquement possible de s'introduire et de contrôler tout système informatique.

Autre exemple révélateur : un établissement bancaire avait installé deux distributeurs automatiques de billets dans deux points de la ville, avec une spécificité : ces distributeurs faisaient uniquement du change (monnaies étrangères). Pas de carte de paiement, mais des billets pour obtenir la devise de votre choix. Chaque début de semaine, la banque s'apercevait que des sommes considérables de billets avaient disparu sans explication et sans échange avec telle ou telle monnaie. Les soupçons s'orientèrent sur tout le monde, depuis les convoyeurs de fonds qui alimentent les distributeurs en fin de semaine, jusqu'aux employés de la banque, soupçonnés d'avoir trouvé un stratagème pour faire telle ou telle chose, en passant par un pirate et ainsi de suite. II n'y avait aucune effraction. En fait, quelqu'un venait chaque veille de week-end dans un hôtel avec un micro-ordinateur et un modem. II s'agissait d'un des techniciens qui avait installé ces distributeurs. II savait que la banque avait demandé que les deux distributeurs soient dotés de modems, afin qu'un employé puisse réactualiser chaque jour les taux de change. La banque avait oublié de changer les numéros de téléphone après l'installation, et aucun mot de passe n'était en place. L'individu se connectait sur la prise de téléphone et, jouant sur la lire italienne, il multipliait le taux de change officiel par un taux plus important, allait récupérer son argent, revenait à son hôtel et remettait par le biais du modem le taux de change officiel... II prenait soin ensuite de retourner dans le fichier qui avait enregistré son appel pour effacer son passage.

Les derniers chiffres révélés par le Pentagone après analyse du fonctionnement des équipes de pirates qui ont pour mission d'attaquer des sites informatiques militaires avec autorisation hiérarchique sont édifiants : ces attaques réussissent dans 88% des cas, seulement 4% des sites attaqués ont repéré ces attaques et moins de 0,5% de celles-ci ont donné lieu à un rapport.

Le premier délit informatique signalé aurait eu lieu aux États-Unis en 1958, mais la première criminalité informatique, identifiée comme telle et poursuivie au niveau fédéral (une altération d'états bancaires à Minneapolis) n'est intervenue qu'en 1966. Dans les pays nordiques, le premier délit informatique poursuivi, un cas de

contrefaçon de logiciel caractérisée, a été commis en février 1968 en Finlande[7]. En général, dans le domaine de la criminalité informatique, les données sous-estiment fortement la réalité. Car lorsque les sociétés sont concernées par des actes illicites, moins d'un tiers d'entre elles le déclarent. Cette répugnance des victimes à dévoiler les défaillances de leurs systèmes informatiques s'explique essentiellement par des raisons d'image commerciale. On la retrouve dans tous les pays touchés par ce phénomène. La peur de la publicité négative et l'inquiétude de communiquer leurs mésaventures à leurs concurrents prenant le dessus sur 1'envie de retrouver 1'auteur de la fraude. Aux États-Unis, seulement 1 à 2% des crimes informatiques sont détectés (d'après le FBI) ; en France, un tiers des pertes n'est probablement pas déclaré. II est clair que le phénomène de la criminalité informatique a des implications économiques importantes, même s'il est parfois difficile de les chiffrer précisément.

Les technologies informatiques et de communication servent également à perpétrer des crimes conventionnels qui étaient jusque-là contrôlables. Par exemple, il est facile, aujourd'hui, de distribuer de la pornographie enfantine par l'intermédiaire des lignes de télécommunication. Cette activité, lorsqu'elle est exécutée à l'échelle internationale, permet de contourner les contrôles douaniers. Tout cela est particulièrement inquiétant, car il est bien connu que les pédophiles profitent de l'anonymat du réseau Internet pour échanger du matériel pornographique. Le même genre de scenario est appliqué pour la transmission de logiciels protégés par des droits d'auteurs, de la littérature haineuse et d'autres documents illégaux.

- Si les forums électroniques sur Internet donnent aux citoyens du monde la facilité de dialoguer à propos de tout et de rien, ils autorisent aussi les malfaisants à se rencontrer voir à s'organiser ou à mettre sur pied des commerces peu licites dans le plus parfait anonymat.
- La tentation est grande pour certains États de contrôler des ressources d'Internet. Selon Vinton Cerf des créateurs du réseau, ce contrôle est techniquement impossible[8]. Essayer de censurer Internet reviendrait à vouloir censurer toutes les communications téléphoniques dans le monde... franchement personne ne pense que ce soit faisable.
- Et le cryptage ? II permet de sécuriser les transactions financières, mais il donne aussi aux malfrats 1'occasion de transférer sans trace et en toute impunité des fonds d'origine illicite.
- L'inspecteur-chef Bryan Drew du National Criminal Intelligence Service du FBI, lors d'une conférence sur « les crimes contre les enfants » a révélé que les réseaux internationaux de pédophiles utilisent de nouvelles techniques de codage pour protéger le secret de leurs communications. Les 3 000 pédophiles

[7]Daniel P., *La police judiciaire contre les crimes sur les systèmes d'information,* in Revue Internationale de Police Criminelle, n°457,1996.

[8] Propos recueillis par Marc Chalamet, Le Parisien du 6 mars 1996

> répertoriés par les services de renseignement britanniques, et branches sur Internet, ont la possibilité de protéger leur messagerie en utilisant une « clé » personnelle pratiquement inviolable. « Il faudrait au moins dix ans à nos ordinateurs opérant en pool pour casser ses codes individuels » précisait Bryant Drew. Les pédophiles échangent ainsi des informations, leurs expériences et des photos qui peuvent être diffusées à des dizaines de milliers d'exemplaires en l'espace d'une journée[9].

La liberté de choix des noms de domaine sur Internet continue à poser de nombreux problèmes juridiques, car tant que l'on applique la règle selon laquelle « le premier arrivé » est « le premier servi», l'usurpation du nom d'autrui apparaît comme une fatalité contre laquelle il est difficile de réagir. Sur Internet, il est fréquent que la dénomination ou la marque d'autrui soit déposée comme nom de domaine.

Avec l'évolution rapide des technologies informatiques et des systèmes d'information et de télécommunication de notre société, une nouvelle forme de criminalité s'est développée : la criminalité informatique.

I.2. La définition de la criminalité informatique

La « *criminalité informatique* » - équivalent de la notion « *fraude informatique*», « *délinquance assistée par ordinateur*», « *criminalité liée à l'informatique*» et « *cybercriminalité* » qui sont presque sur toutes les lèvres.

Dans les ouvrages et documents qui traitent de la criminalité informatique, nous trouvons de très nombreuses définitions, dont certaines sont restreintes et précises, et d'autres larges et générales. Nous retenons la définition de Donn B. Parker[10]qui a été adoptée par le ministère de la justice des États-Unis et selon laquelle la criminalité informatique est « *tout acte illicite nécessitant une connaissance spécialisée de l'informatique, au stade de la perpétration, de l'enquête de la police ou des poursuites pénales* ». Plus tard, un groupe d'experts réuni dans le cadre de l'Organisation de coopération et de développement économique(OCDE) a adopté cette autre formulation : « *l'abus informatique est tout comportement illégal, contraire à l'éthique ou non autorisé, qui concerne un traitement automatique et /ou une transmission de données*[11]». Dans le cadre de ses travaux sur ce sujet, l'OCDE a retenu plusieurs caractéristiques de la criminalité informatique :

---

[9] Pour savoir de plus, voir les reportages : *la protection des signes distinctifs d'Interpol*, la Semaine juridique, 20/05/1998

[10] Ministère de l'intérieur de la France, *la criminalité informatique à l'horizon2005*, FORS, Paris, octobre, 1991, P42.

[11] OCDE, *la fraude liée à l'informatique :analyse des politiques juridiques*, Paris, 1986, P62.

- L'entrée, l'altération, l'effacement et /ou la suppression des données et des programmes dans l'intention de commettre un transfert illégal de dons, de commettre un faux ou d'entraver le fonctionnement du système informatique et /ou de télécommunication ;
- La violation du droit exclusif du détenteur d'un programme informatique protégé dans l'intention de l'exploiter commercialement et de le mettre sur le marché ;
- L'accès dans un système informatique et/ou de télécommunications ou l'interception d'un tel système fait sciemment et sans l'autorisation du responsable du système, en violant les règles de sécurité ou dans une intention malhonnête ou nuisible.

Toutefois, l'impossibilité de parvenir à une définition internationale a pour résultat de créer des difficultés pour connaître l'étendue réelle de cette fraude et pour en mesurer le volume économique. En 1989, le Conseil de l'Europe a retenu une approche plus formelle sur la criminalité informatique[12], en proposant une liste minimale et une liste facultative des délits informatiques qui devraient être réprimés dans le cadre des législations européennes.

I.3. Le poids du cyber crime

À l'absence d'instruments de mesure précis, le coût global du monde entier de la criminalité informatique demeure une inconnue. Les formes de phénomène criminel et des risques liés aux technologies informatiques en général diffèrent selon les pays, la recherche des facteurs explicatifs de ces clivages demeure au stade des hypothèses. Les comparaisons internationales sont très difficiles à établir, les données exhaustives étant peu homogènes, voire inexistantes.

Bien qu'il soit difficile de connaître avec précision l'ampleur réelle de la criminalité informatique, les enquêtes et les estimations réalisées par certains organismes permettent de dégager les principales caractéristiques de la criminalité au niveau mondial. La dépense informatique mondiale est très concentrée : plus de la moitié aux États-Unis, environ 30% en Europe et près de 10% au Japon.[13] Les risques potentiels et le montant des pertes dus à la criminalité informatique sont donc également très concentrés. Il semble que la hiérarchie des risques corresponde au degré d'informatisation.

---

[12] *Politique de lutte contre la criminalité liée à l'ordinateur en Europe et nouvelles formes de criminalité informatique,* rapport du dr. Manfred, Mohrenschiager présenté lors de la Conférence organisée conjointement à Luxembourg par le Conseil de l'Europe et la Commission des Communautés européennes, le 27 mars 1990, P.82.

[13] Presses Universitaires de France, *Criminalité informatique (Que sais-je ?) Paris, 1988, P 243).*

Selon les estimations communiquées en France par le Centre de documentation et d'information de l'assurance (CDIA), la proportion[14] des pertes provoquées par des accidents ou des malveillances dans l'exploitation des moyens informatiques par rapport aux pertes globales est passée de 37% en 1985 à 58% en 1994, et ceci pour un montant évalué actuellement à 6,4 milliards de francs français. Le nombre de fraudes informatiques signalées aux services de police judiciaire est très inférieur à celui connu des sociétés d'assurances et présenté chaque année par le Centre de documentation et d'information de l'assurance CDIA.

Les résultats de l'analyse réalisée par la police belge, vient de rendre public les chiffres inquiétants de la cybercriminalité**,** Publié le 16/10/2019 par Etienne Wery. Dans un rapport statistique 2017-2018 de la criminalité, un chapitre spécial est consacré aux « hausses remarquables » à commencer par la criminalité informatique. Sur ce point, l'année 2018 a été catastrophique avec une augmentation de 14,8 %.
Quelles sont les infractions reprises dans les statistiques ?

La Loi relative à la criminalité informatique comprend 4 infractions (hacking, faux en informatique, fraude informatique et sabotage) :

- Le hacking, également appelé «piratage informatique», consiste à se procurer illégalement un accès à un système informatique (hacking externe) ou à outrepasser son autorisation d'accès (hacking interne), y compris les actes préparatoires, le hacking sur demande (donner l'ordre ou inciter à) et le recel des données obtenues par le biais du hacking. Par exemple: s'introduire dans le réseau d'une entreprise dans le cadre d'un espionnage industriel ou se donner accès au compte e-mail d'une autre personne. 3 575 faits de hacking ont été enregistrés en 2018, ce qui représente une augmentation de 986 constatations par rapport à 2017.
- Le faux en informatique consiste à changer la portée juridique de données par l'introduction, la modification ou l'effacement de données ou par la modification de l'utilisation normale des données du système informatique. Par exemple la falsification d'une carte de crédit ou la création d'un faux profil (p. ex. Facebook, Netlog, etc.) au nom d'une autre personne. Les faits de faux en informatique ont augmenté pour atteindre 1 189 enregistrements en 2018.
- La fraude informatique vise à s'approprier indûment un avantage économique par l'introduction, la modification ou l'effacement de données ou par la modification de l'utilisation normale des données du système informatique, par exemple en bloquant l'ordinateur d'une personne par le biais d'un malware. La fraude informatique augmente de 10,2% (+ 1 786 faits).
- Le sabotage informatique consiste à causer des dégâts par l'introduction, la modification ou l'effacement de données ou par la modification de l'utilisation normale des données du système informatique alors que l'on sait que l'on n'est pas

[14] Daniel P.., *La police judiciaire contre les crimes sur les systèmes d'information,* in Revue Internationale de Police Criminelle, n°457,1996.

autorisé à le faire, par exemple répandre un virus. Seul le sabotage peut être crédité d'un statu quo dans la tendance constatée.

Le Moniteur de sécurité (enquête à grande échelle organisée par la Police fédérale au cours de laquelle la population belge est questionnée à propos de différents thèmes en matière de sécurité) a sondé les répondants sur différents faits concernant l'internet, parmi lesquels la possibilité d'avoir été victime d'un délit dans le courant des 12 derniers mois :

- L'escroquerie sur internet 8,14% des citoyens rapportent avoir été au moins une fois victimes de ce type de fait au cours des 12 derniers mois (au moment de l'enquête) et 21,58% d'entre eux déclarent avoir porté plainte. Cela signifie qu'il y aurait près de 5 fois plus d'escroqueries sur internet que ce que le nombre des procès-verbaux laisse à penser. Autrement dit, le chiffre noir serait d'environ 82%.
- L'intrusion dans un ordinateur ou smartphone 7,82% des citoyens déclarent avoir été au moins une fois victimes de ce type de fait et 13,61% d'entre eux rapportent avoir porté plainte pour ce fait. Autrement dit, 86% des intrusions dans un ordinateur ou un smartphone ne seraient pas connues des services de police. Le rapport insiste sur le fait qu'il est important de soulever la notion de connaissance ou la conscience de ces intrusions. On peut se demander dans quelle mesure le citoyen sait qu'il est victime d'une intrusion dans son ordinateur ou smartphone. Si l'on considère que les citoyens n'ont pas conscience de ce délit dans nombre de cas, le chiffre noir est d'autant plus important.
- L'intimidation et le harcèlement via internet 3,34% des citoyens interrogés rapportent avoir été au moins une fois victimes d'un tel fait au cours de ces 12 derniers mois. Parmi ceux-ci, 22,31% des citoyens rapportent avoir porté plainte pour ce fait. Cela signifie qu'on peut estimer qu'environ 78% de ces faits ne sont pas rapportés à la police. Outre les précautions à prendre comme pour toute estimation du chiffre noir, il faut ici également garder à l'esprit la subjectivité des notions d'intimidation et de harcèlement et donc prendre d'autant plus de précaution quant à cette estimation.

Les données du Moniteur de sécurité révèlent des taux de déclaration à la police relativement faibles pour les délits dont les citoyens ont été victimes sur internet. Le rapport tient comme explication probable le fait que les citoyens ne perçoivent pas/plus l'intérêt, l'utilité ou encore l'importance de déclarer de tels faits. L'anonymat des auteurs et la difficulté à les retrouver peut décourager le dépôt de plainte. La banalisation de certains faits (p.ex. harcèlement sur internet) pourrait aussi expliquer ce taux de plainte assez faible.

II. LA TYPOLOGIE DES CRIMINELS ET LEURS MOTIVATIONS

La criminalité informatique est essentiellement orientée vers le profit, mais sans pour autant que tous les criminels informatiques aient des motivations similaires. D. Parker en distingue ainsi 7 catégories (types) de cyber crimes et de cybercriminels[15]:

- La première catégorie est celle *des « amateurs* », les plus nombreux, sont des criminels informatiques, détenant précisément ces postes de confiance grâce à un certain niveau de connaissances des techniques informatiques. Le plus souvent, ils commettent un délit à cause de problèmes financiers, afin de compenser des difficultés professionnelles ou pour satisfaire leurs penchants égoïstes.
- La deuxième catégorie de criminels informatiques regroupe *les « détraqués »* ; ils utilisent la violence et souffrent du déséquilibré psychologique plus ou moins grave.
- La troisième catégorie de criminels informatiques concerne *le crime organisé* qui pourrait s'intéresser à l'informatique, car les gains potentiels sont importants et les risques moins élevés que dans ses activités traditionnelles. Mais les cas sont relativement peu nombreux, soit parce que la mafia a encore peu investi dans le crime informatique, soit parce qu'elle ne s'est pas fait prendre. Mais lorsqu'elle utilise l'informatique, il s'agit d'opérations criminelles de grande envergure.
- *Les Puissances étrangères* forment la quatrième catégorie de criminels informatiques : les motivations essentielles sont l'espionnage ou le vol de secrets commerciaux.
- *Les Criminels professionnels* constituent la cinquième catégorie qui, n'appartenant pas au crime organisé, sont également peu nombreux à commettre des délits informatiques, car relativement marginalisés, ils ont plus rarement des opportunités. II leur est plus difficile d'assimiler les techniques informatiques et ils préfèrent souvent exercer des activités plus classiques (hold-up, racket, trafic de stupéfiants...). Les cas connus concernent essentiellement des escroqueries effectuées à l'aide d'ordinateurs.
- La sixième catégorie regroupe les *«casseurs de systèmes».* Ils utilisent les failles dans les procédures d'accès aux systèmes informatiques. La perfidie ou la supercherie ne seraient pas nécessairement à l' origine de la fraude ; ils cherchent tout simplement à atteindre un but, sans vouloir en tirer profit, tout simplement« pour se faire plaisir ». Ce ne sont pas forcément des professionnels. Beaucoup d'entre eux sont des collégiens, ou des étudiants.

[15] https://www.faronics.com. *7categories de criminels informatique.* Poster par ASMITH 3/11/2020. Consulté le 14/10/2022 à 15h00.

- La septième et la dernière catégorie rassemble les *« extrémistes idéalistes»*, essentiellement des groupes terroristes.

Une typologie plus sommaire est proposée par Bologna[16] qui distingue les comportements des criminels informatiques:

- Économiques (recherche de gains financiers),
- Egocentriques (la recherche de reconnaissance sociale, le gain n'étant pas primordial),
- Idéologiques (revanche sur la société) et
- Psychotiques caractérisés par la perte du sens des réalités.

En fait, selon Philippe Rose[17], quel que soit le degré de précision des typologies et leurs dénominations, les motivations essentielles correspondent à quatre catégories de criminels informatiques :

- Tout d'abord, les « utilitaristes » qui ont pour objectif le gain financier ; ils effectuent principalement des détournements de fonds.
- Ensuite, les « entrepreneurs » agissent par jeu ou par défi en pénétrant les réseaux et les systèmes informatiques. Ils pratiquent le piratage des logiciels et des données et sont spécialistes de la recherche des mots de passe. Ils contestent leur assimilation aux autres criminels informatiques, se considèrent inoffensifs et affirment utiliser un code de déontologie(ne pas créer de dommages aux systèmes qu'ils pénètrent).
- Les « agressifs », la troisième catégorie, agissent guidés par le désir de compenser une frustration personnelle ou professionnelle. Ils utilisent les bombes logiques, les chevaux de Troie, les virus, le vol des données et des fichiers.
- Enfin, les « destructeurs » ont pour but de nuire aux entreprises ou organisations auxquelles ils s'attaquent par le sabotage ou le terrorisme.

II est évident que le criminel informatique n'a pas une motivation unique, ses objectifs sont souvent variés et complémentaires. Les typologies ne font que suggérer un découpage possible ; les frontières entre les différentes catégories de criminels sont souvent difficiles à établir.

---

[16]BOLOGNA G.., *An Organizational Perspective on Enhancing Computer Security,* Communication au Congres Securicom, 1986.
[17]PHILIPPE R., *Criminalité informatique*, (Que sais-je ?), Paris : Presses universitaires de France, 1988. P. 32

III. LA CRIMINALITÉ INFORMATIQUE LA PLUS FRÉQUENTE

Les statistiques nationales et internationales, et sur les informations officieuses qui circulent, on constate que les cas les plus connus et les plus fréquents sont les piratages informatiques (activités des « hackers »), les piratages téléphoniques, les modifications des logiciels et des données et la pédophile sur Internet.

III.1. Piratage informatique

Le piratage informatique est également appelé souvent «intrusion » et « hacking ». C'est une pratique consistant à entrer par effraction dans un réseau informatique en forçant ou en contournant les dispositifs de sécurité d'un ordinateur. Le piratage n'est pas à prendre à la légère, la plupart des principaux systèmes informatiques dans le monde étant connectés à des réseaux.

La définition de cette infraction est la suivante : « accès non autorisé à un système ou un réseau informatique ». « Accès » signifie « intrusion dans tout ou partie d'un système et des programmes ou données qu'il contient». La méthode de communication importe peu : l'accès peut être local et direct ou à distance et indirect, par exemple via une liaison satellite ou d'autres systèmes informatiques. Les pirates utilisent fréquemment des messageries ou serveurs télématiques permettant des échanges d'informations entre utilisateurs. En échangeant des numéros informatiques à composer et en profitant de mots de passe périmés et d'autres failles dans les systèmes informatiques, ils peuvent avoir accès à des systèmes informatiques et obtenir des informations précieuses. Dans le cadre de leurs activités, ils ont inventé un nouveau jargon ou langage et utilisent des pseudonymes pour dissimuler leur véritable identité.

Le piratage constitue une infraction spécifique dans certains pays, alors que dans d'autres, la législation traditionnelle en vigueur est invoquée pour traduire les auteurs en justice. Certains considèrent cette pratique comme un jeu ou un passe-temps, mais les victimes la prennent au sérieux. Puisque parfois, le piratage ou l'accès non autorisé à des systèmes informatiques constitue la première étape d'une infraction plus grave, telle que l'espionnage ou le sabotage. Devant la conférence des ambassadeurs, le 28 août 1998, un commissaire de la DST, Daniel Martin[18], évoque des cas tout récents d'attaques de systèmes informatiques par des groupes organisés de pirates. En mai, une équipe de « hackers » âgés de quinze à dix-huit ans, The Milworm, est ainsi entre dans le réseau d'un centre de recherches atomiques indien et y a volé des travaux sur les derniers essais nucléaires ordonnes par les autorités de New Dehli. En Août, des partisans des Tigres tamouls, rebaptisés pour l'occasion les Tigres noirs de l'Internet, ont lancé une attaque contre le réseau reliant les ambassades du Sri-Lanka, bloquant les

[18] *Voir Dossier Délinquance, Le Monde, 22/09/1998.*

boîtes aux lettres électroniques de toutes ses représentations dans le monde. En Septembre, les messages émis par le service de sécurité du président des États-Unis ont été diffusés sur un serveur Internet.

Une autre sorte de piratage informatique consiste à entrer illégalement sur le serveur web et à modifier les pages existantes. Ce faisant, en Mai 1996, un office spécialisé du Sénat des États-Unis avertit: « des entités hostiles peuvent s'emparer de systèmes d'information de la Défense, affectant gravement notre capacité à déployer et soutenir nos forces armées ». II signale aussi 162 500 infiltrations réussies dans les ordinateurs de la Défense nationale américaine en 1995[19].

III.3. Piratage téléphonique[20]

Le piratage téléphonique est souvent appelé *phreaking* en anglais. II peut se décrire comme le détournement de services de télécommunication par divers procédés, dans le but d'éviter les grosses factures de téléphone ou les oreilles indiscrètes. Autrement dit, le piratage téléphonique est un : « Accès non autorisé à des services de (télé) communication, obtenu sans respecter les protocoles et les procédures». Les premiers cas de piratage téléphonique recensés remontent aux années 60. À cette époque, le piratage informatique était une activité essentiellement pratiquée par des adolescents qui savaient obtenir la tonalité et passer gratuitement un appel local d'une cabine téléphonique en provoquant un court-circuit au moyen d'une pince ou d'une épingle à cheveux placée entre le microphone et le monnayeur. Ils connaissaient aussi certainement d'autres moyens de passer des appels téléphoniques sans payer.

La commutation des lignes utilise des fréquences vocales que l'on peut reproduire avec un ordinateur et une carte sonore. Petit à petit les techniques se sont perfectionnées, Le premier véritable outil des pirates c'est ce qu'on appelle en anglais le *boxing*, une petite boîte remplie de composants électroniques qui permettant de reproduire exactement cette fréquence, soit 2600 Hz, c'est-à-dire, de Fagon générale, l'utilisation d'équipements électroniques dans le but de leurrer les centraux téléphoniques. Les « boîtes »(boxes) génèrent des signaux sonores qui trompent le central, et celui-ci répond par exemple en libérant des lignes ou en arrêtant le compteur d'unité.

Les pirates ont inventé différents types de « boîtes » (boxes), désignés chacun par sa couleur[21]. La boîte noire comporte un ou deux interrupteurs ; elle est

---

[19]Daniel M., *la criminalité informatique*, Presse universitaires de France, avril 1997, Paris.
[20]Raymond Mc G., *la fraude aux télécommunications*, in Revue internationale de police criminelle, n°464, Paris 1997, P 29.

[21]Raymond M., *la fraude aux télécommunications*, in Revue internationale de police criminelle, n°464, Paris 1997, P 17.

reliée à la ligne téléphonique du destinataire de l'appel et permet de lui téléphoner gratuitement. L'activation de la boite supprime le signal qui indique que le destinataire de l'appel a décroché et qui déclenche le compteur. La boîte blanche (cheese box) permet de mettre en relation deux personnes qui appellent deux numéros différents correspondant au même local. Un correspondant appelle un des deux numéros et reste en communication tandis que la deuxième personne appelle l'autre numéro, la communication étant établie entre les deux intermédiaires de la boîte blanche (cheese box). La boîte rouge permet de générer des signaux identiques à ceux qui sont émis lorsque l'usager d'une cabine publique introduit des pièces dans la fente de ma machine. La boîte violette reliée à la ligne d'une personne qui passe des appels à longue distance, envoie au central téléphonique le même signale que s'il s'agissait d'un appel local, de telle sorte que l'appelant n'a pas à payer le prix des communications à longue distance.

La « boîte » la plus répandue est la « boîte bleue ». Elle existe depuis longtemps déjà, mais elle a été modifiée et perfectionnée au cours des années. Le pirate compose un numéro et à l'aide de sa boîte bleue, génère un signal à 2600 Hz juste au moment de la connexion. Ce signal trompe le central téléphonique local en lui indiquant que la communication est terminée. Le pirate compose alors sur sa boîte bleue le numéro du correspondant auquel il veut parler, et la communication est établie. Le central interprète cet appel comme provenant d'un autre central et ainsi la communication n'est pas facturée au pirate[22].

Un autre moyen simple de frauder consiste à obtenir les codes permettant de passer des appels à longue distance. Lorsque ces codes ont été introduits, ils comportaient seulement six à huit chiffres. Ils pouvaient être piratés soit manuellement à partir d'un téléphone à touches, soit par des moyens informatiques, à l'aide d'un ordinateur et de logiciels conçus à cet effet. II est possible de se procurer ces codes en appelant le numéro d'accès propre à chaque compagnie de téléphone, en essayant un code puis en composant le numéro du correspondant; si la communication est établie, c'est que le code utilisé était le bon.

Un autre type de piratage téléphonique est l'utilisation détournée des téléphones cellulaires. Avec ce type de téléphones, aucune connexion physique n'est nécessaire, et il est facile d'écouter les conversations au moyen de scanners, les téléphones cellulaires sont aussi facilement reprogrammables : les malfaiteurs peuvent ensuite les utiliser sans payer leurs communications, qui seront facturées aux véritables propriétaires.

[22] https://fr.m.wikipedia.org. *Blue box dispositif pirate pour réseaux téléphoniques.* Consulté le 14/10/2022 à 17h15.

III.3. Modification de logiciels ou de données

II s'agit des insertions de programmes malveillants. L'objectif est d'altérer des données ou des programmes, ou de gêner leur utilisation, en mettant de ce fait en péril l'intégrité ou la confidentialité du système lui-même ou de ses sorties.

III.3.1. Les virus informatiques

Les virus informatiques sont des programmes informatiques qui se reproduisent jusqu'à paralyser le fonctionnement normal de l'ordinateur. Ils infectent discrètement les programmes sur disques et peuvent être difficiles à déceler. Les conséquences d'un virus peuvent aller de la simple farce à la destruction complète des données. Les utilisateurs propagent souvent involontairement les virus lors des opérations quotidiennes telles que l'utilisation d'un disque sur plusieurs machines. II existe à l'heure actuelle des milliers de types de virus informatiques[23]. Chacun a ses caractéristiques propres, mais tous altèrent les fichiers de données ou les programmes. Mais plusieurs catégories de virus informatiques ont été analysées par des fonctionnaires de police spécialisés ou des professionnels indépendants. De ce fait, la plupart des virus peuvent être facilement décelés et des remèdes être trouvés. Les virus informatiques sont de véritables entités internationales. Ils se transportent de toute évidence d'un ordinateur à l'autre et d'un pays à l'autre. Les modes de propagation des virus informatiques sont principalement suivants : logiciel informatique piraté ou illicite, logiciel partagé, disquettes offertes par les revues informatiques, logiciel non breveté, jeux informatiques, souvent copiés dans les écoles et les lycées et l'utilisation de messageries ou serveur télématiques et le téléchargement des données comportent un risque élevé d'infection par virus.

III.3.2. Cheval de troie[24]

Cette infraction est une: « altération non autorisée de données ou de programmes informatiques par l'insertion d'un Cheval de Troie». Le Cheval de Troie est un programme dissimulé dans un système informatique. Contrairement aux virus informatiques, le Cheval de Troie ne se multiplie pas nécessairement. II consiste à ajouter quelques lignes d'instructions dans un programme existant qui ont pour résultat de faire exécuter par l'ordinateur des opérations non programmées. Très souvent, une «trappe» est pratiquée, permettant l'accès non autorisé à un programme ou un ordinateur. Les pirates l'utilisent fréquemment pour se ménager une entrée dans les

[23] Les experts en virus estimaient qu'il existait près de 6500 virus et que chaque jour il en apparaissait deux ou trois. *Le Guide clandestin de la sécurité des ordinateurs* écrit par Michael Alexander, International Thomson Publishing France, Paris, 1997, p.33.

[24] https://fr.wikipedia.org. « Cheval de troie » consulté le 29 septembre 2022 à 13hoo.

systèmes en mettant les mécanismes de protection en échec et en se servant d'un accès au moyen d'un code secret. L'affaire de la « disquette du SIDA» (1989) en constitue un exemple. 20000 disquettes contenant un programme d'information sur le SIDA et contenant aussi un programme caché qui, modifiant l'un des fichiers du système, ont été envoyées de par le monde, dans un emballage faisant croire qu'elles provenaient de l'OMS. Lors de l'utilisation du programme, le traditionnel texte de la licence s'affiche, mettant en garde l'utilisateur contre l'utilisation frauduleuse du logiciel et l'invitant à payer le logiciel. Et en fait, lorsque l'utilisateur lançait le programme, un compteur caché démarrait qui, lorsqu'il atteignait 90, chiffrait tous les fichiers de données et rendait 1'ordinateur inutilisable.

III.3.3. Bombe logique[25]

Celle-ci désigne: « altération non autorisée de données ou de programmes informatiques par l'insertion d'une Bombe logique.» La Bombe logique est un mécanisme logique introduit par les malfaiteurs, qui se déclenche lorsque l'ordinateur exécute une tâche donnée. Une fois déclenché, le mécanisme lance un petit programme dont l'exécution affecte le fonctionnement de l'ordinateur ou du réseau de différentes manières : arrêt complet de l'ordinateur, affichage de pages d'écran vierges, destruction de données, etc. II s'agit du nom donné à la pratique illicite consistant à introduire une simple modification dans le code source du programme, qui déclenchera un processus de destruction. La bombe logique sera activée par une date ou par un évènement particulier, qu'il y ait présence ou absence des données. Les auteurs de la bombe logique sont généralement eux-mêmes programmeurs.

III.3.4. Les vers[26]

Les vers sont des programmes destructeurs analogues aux virus, qui sont créés pour les réseaux informatiques et altérer des données. Ils se reproduisent intégralement en créant des copies conformes d'eux-mêmes.

On les trouve dans les réseaux informatiques et les ordinateurs sur lesquels travaillent plusieurs utilisateurs. Ils se déplacent en utilisant les communications inter ordinateurs comme moyen de transport. Ils sont en général conçus pour s'attaquer aux gros systèmes informatiques. Les vers se rencontrent peu; ils sont moins fréquents que les virus.

L'affaire la plus connue et la plus dévastatrice est le ver d'ARPANET. Le 2 novembre 1988, un étudiant de l'université de Harvard a lancé un ver sur le réseau ARPANET. Le ver s'est transmis de machine en machine grâce à une faille dans le

[25] https://www.avast.com. «qu'ets-ce qu'une Bombe logique ? Exemple et prévention-Avast » consulté le 29/9/2022 à 16H00.
[26] https://www.websecuriy.digicert.com. «Différents virus informatiques » consulté le 29/9/2022 à 16H5.

système de messagerie électronique. Le ver sature les machines contaminées en se reproduisant très vite, l'ensemble des communications sur le réseau est très fortement ralenti. Les administrateurs systèmes n'ont pas eu d'autres choix que de déconnecter leurs machines du réseau.

III.4. La pédophilie sur internet[27]

Actuellement, Internet jouit d'une immense popularité. II est généralement admis qu'entre 50 et 90 millions de personnes, disséminées un peu partout dans le monde, utilisent le réseau Internet. Or l'intégration de ce mode de communication à la culture populaire accroît le risque qu'il soit utilisé à mauvais escient. Le réseau Internet, qui est un réseau à longue distance, ou plus précisément une infrastructure permettant le transport des données, a été conçu pour échanger efficacement des informations sur le plan international. Ce réseau est mondial et ne connait pas de frontières. II est très difficile à contrôler et constitue, par conséquente, un moyen de dissimulation très efficace pour les utilisateurs. Les malfaiteurs, qui ont très vite découvert ses avantages, ont décidé de l'utiliser pour des activités illégales. La pédophilie est un exemple particulièrement saisissant de criminalité ayant pris de l'ampleur grâce à Internet. L'exploitation des enfants à des fins sexuelles est un problème mondial. Ainsi, estime-t-on que l'industrie du sexe fait plus d'un million de nouvelles victimes chaque année. Selon une étude menée par la Carnegie Mellon University, à Pittsburgh, en Pennsylvanie, la diffusion d'images à caractère sexuel constitue l'une des plus importantes activités criminelles utilisant les réseaux informatiques. Pendant longtemps, les pédophiles opéraient dans des cercles assez restreints[28]. Désormais, ils ont la possibilité d'offrir ou d'acquérir du matériel photo ou vidéo dans le monde entier. Et cela, juste en pianotant sur le clavier d'un ordinateur.

Les pédophiles peuvent y reproduire des informations ou des photos, Internet est en fait apparu très insidieusement, l'anonymat y est préservé, la distribution de documents est simple et la quantité des matériaux que le réseau peut transporter est sans limite. Depuis quelques temps, on constate un accroissement des forums qui s'adressent aux pédophiles en leur offrant des adresses, des informations ou tout simplement des images. Ces échanges d'informations sont faciles grâce à Usenet, une sorte de messagerie implantée dans Internet. Au lieu d'envoyer un message à une personne, l'utilisateur participe à des « newsgroups » sur des thèmes particuliers. Selon le Groupe de travail de recherche, sur 25.000 « newsgroups », 0,07% contiennent des

---

[27] Conférence des évêques de France « *Le guide élaboré pour la pédophilie »* (Ed. Bayard-Cerf-Mame - 9 euros) a été mis à jour en janvier 2017.

[28] RICHARD P. *La mondialisation du marché du sexe* dans Actuel Marx 2002/1 (n°31), France, P. 109-122

matériaux pédophiles. Rien qu'en janvier 1998, 6.000 photos pédophiles ont ainsi été diffusées[29].

Avec le web, les réseaux de pédophiles s'étendent sans souci qui des frontières ni des législations. Sur Internet, certains sites sont de véritables « boutiques porno virtuelles ». Selon des spécialistes, il y a plus de 5.000 sites de pornographie, ce chiffre étant en augmentation constante. Beaucoup sont protégés par une diversité de logiciels de cryptage estimés à quelques 350 logiciels en libre circulation. En outre, une enquête réalisée en 1994 aux États-Unis en vient à la conclusion que le réseau Internet renfermait alors plus de 450 000 images ou fichier-textes de nature tomographie[30]. En fait, les sites pédophiles se sont multipliés aussi sur Internet. Ces sites ne sont pas pour autant accessibles au premier internaute venu. On ne s'y retrouve jamais par hasard, pour les atteindre, et surtout y rester, il faut s'entourer des précautions : pseudonyme, mots-clés, langage codé, numéros de carte bancaire,... Les intrus ont tôt fait d'être repérés et « expulsé » par les habitués du lieu.

IV. PISTES DE SOLUTION

Cet article ne se base pas seulement, à dresser un panorama de criminalité informatique, analyser les comportements et les outils utilisés par des malfaiteurs, mais aussi expose les pistes des solutions, les moyens techniques pour la protection et la prévention contre cette menace informatique :

IV.1. La protection technique contre les pirates

Les ordinateurs renferment de plus en plus de secrets personnels, professionnels et étatiques. Les médecins leurs confient des informations médicales sur les patients ; les entreprises, leurs données stratégiques ; les banques, les comptes de leurs clients,... Mais ces données sont-elles bien protégées ? On peut en douter quand on constate le formidable essor du piratage informatique :

- Protection par mot de passe contre les pirates : Une des manières principales de limiter ou de contrôler l'accès à une machine est d'utiliser des mots de passe, mais tous les utilisateurs d'ordinateurs n'en saisissent pas réellement l'importance. Les mots de passe sont très importants parce que c'est la première ligne de défense contre les attaques sur un système. Ceci peut être établi simplement: si un hacker ne peut pas interagir sur un système distant et qu'il ne peut pas ni lire ni écrire dans

[29] Souheil EL ZE IN, *l'indispensable amélioration des procédures internationales pour lutter contre la criminalité liée à la nouvelle technologie*, Paris 1998, P. 32.
[30] https://www.lemonde.fr*Impossible censure des sites pornographiques – Le monde.* Consulté le1 septembre 2022

le fichier des mots de passe, alors il n'a quasiment aucune chance de développer une attaque couronnée de succès sur ce système.

- Le cryptage[31] : une arme contre le piratage informatique :

La protection par simple mot de passe n'est quelquefois pas suffisante. Pour éviter les risques d'insécurité informatique, établir des barrières de sécurité et combattre les dangers, les experts estiment qu'un meilleur moyen est vraiment efficace : le cryptage[32] : Cette opération consiste à rendre les fichiers informatiques d'un utilisateur illisibles pour un autre utilisateur.

- L'installation d'une paroi anti feu ou pare-feu (firewall)[33]. La paroi anti feu, en anglais firewall, fournit une protection digitale associée à la rapide croissance des réseaux et de la commercialisation de l'Internet. Beaucoup de gens ont entendu parler des firewalls, mais peu de personnes les utilisent. De plus, le nombre d'incidents de sécurité grandissant sur Internet laisse suggérer très fortement que trop peu de personnes les utilisent correctement. La paroi anti feu est une sorte de technologie de contrôle d'accès qui empêche les accès non autorisés aux ressources d'information en plaçant une barrière entre le réseau de l'entreprise et le réseau non-sécurisé (Internet, par exemple).

IV.2. Éradiquer les virus informatiques

II y a toutes sortes de programmes informatiques capables de détruire des données ou des systèmes : les virus, les Chevaux de Troie, les bombes logiques, etc. II ne faut pas les sous-estimer. La seule manière d'être sûr qu'un virus est la cause des problèmes, passe par l'utilisation d'un logiciel antivirus. En général, il y a quatre procédés qui permettent la détection et l'éradication des virus: le *scanner*, *le détecteur de changement des fichiers, le détecteur d'activité des virus*, *et le désinfectant.* La plupart des logiciels antivirus vendus offrent une combinaison de ces procédés.

IV.3. Contre la cybercriminalité[34]

Comme chaque pays a une législation différente au sujet de la criminalité, chaque gouvernement devrait, à travers les tenants des maisons de télécommunication, contrôler les matières publiées ou postées à l'internet, afin de limiter ou bannir les obscénités (pédophilie, pornographie, etc) et des programmes endommageurs des informations protégées.

---

[31] https://fr.m.wikipedia.org*Chiffrement ou cryptage.* Consulté le 1 octobre 2022 à 12h20

[32] ZIMMERMANN P., *Cryptographie et réseau, Pour la science*, Paris, juin 1999.

[33] https://solutions.lesechos.fr PEM : *Comment se protéger du piratage Informatique*. Consulté le 1 octobre 2022 à 12h35

[34] BRIGITTE P., *La lutte contre la cybercriminalité : de l'abondance de norme à sa perfectibilité,* dans Revue Internationale de droit économique 2016/3 P. 387-409.

IV.4. L'harmonisation et la Coopération Internationale

La nécessité d'une étroite harmonisation internationale dans ce domaine résulte surtout de la grande mobilité des informations dans les systèmes informatiques. Cette mobilité des données rend possible la perpétration d'une infraction au moyen d'un ordinateur dans un pays pendant que le succès de cet acte criminel se réalise dans un autre pays. Ainsi, de tels délits demandent-ils une coopération internationale effective qui est aussi essentielle pour une protection effective des systèmes de télécommunication traversant plusieurs pays. L'exportation des programmes informatiques à l'étranger justifie aussi la nécessité d'une règlementation juridique internationale.

CONCLUSION

Les problèmes qui sont évoqués à travers la criminalité informatique sont loin d'avoir trouvé une solution. En guise de conclusions, nous avons essayé de mettre en valeur les éventuels obstacles et difficultés que rencontrent les professionnels dans la lutte contre la criminalité informatique et soulever certaines questions. Jusqu'à présent, dans la plupart des pays, seuls les objets corporels et visibles sont protégés par les lois. Bien que la sauvegarde des informations et les autres biens immatériels existent aussi depuis quelques temps dans quelques pays, elle était moins importante. Aujourd'hui, ce point de vue a changé. Ces types d'infractions informatiques sont entre autres: les cas des intrusions informatiques, des piratages téléphoniques, des virus informatiques, drones assistés par l'informatique et la pédophilie sur Internet.

Pour mieux se protéger des pirates, mieux vaut bien les connaître. Donc, il est indispensable de savoir les motivations, les techniques, les comportements et les moyens des criminels informatiques pour établir les mesures techniques et juridiques de protection et de prévention susceptibles de réduire les risques. La prévention et la lutte contre la criminalité informatique pose une série de problèmes techniques, juridiques et de coopération internationale. Mais, cela ne concerne pas seulement la police judiciaire, la prise sociale de conscience de l'importance de la sécurité informatique à tous les niveaux de la société est extrêmement important. Donc nous tous, les habitants qui vivons dans un espace virtuel, devons maîtriser certains rudiments de la sécurité informatique. Chaque pays est appelé à s'impliquer dans cette lutte contre le cyber criminalité, via les tenants de la télécommunication ou des réseaux sociaux. Pour y arriver, il est nécessaire d'élaborer des lois relatives à la protection de l'information et à la peine contre la criminalité informatique au niveau mondial.

BIBLIOGRAPHIE

Ouvrages

AKTOUF O. (1992), *Méthodologie des sciences sociales et approche qualitative des organisations,* PUO, Québec.

ALEXANDER M. (1997), *Le guide clandestin de la sécurité des ordinateurs*, International Thomson Publishing France, Paris.

Martin D. (1997), *La criminalité informatique*, Paris : Presse universitaires de France.

N'DA P.(2002), *Méthodologie de la recherche, de la problématique à la discussion des résultats,* Éditions Universitaires de Côte d'Ivoire, Abidjan.

PARKER D.-B. (1958), *Combattre la criminalité informatique*, Paris, Ed. Oros.

ROSE Philippe. (1988), *Criminalité informatique*, Paris : Presses universitaires de France.

Articles

BRIGITTE Pereira, (2016), *La lutte contre la cybercriminalité : de l'abondance de norme à sa perfectibilité,* dans Revue Internationale de droit économique.

DANIEL PADOIN**,** (1996), *La police judiciaire contre les crimes sur les systèmes d'information*, Revue Internationale de Police Criminelle, n°457.

DANIEL Martin, (1997)*La criminalité informatique,* Presse universitaires de France, Paris.

O.C.D.E.(1986)**,***La fraude liée à l'informatique* : analyse des politiques juridiques, OCDE, Paris.

Bologna G.-J. (1986), *An Organizational Perspective on Enhancing Computer Security*, Communication au Congres Securicom.

RAYMOND Mc Governa (1997)*La fraude aux télécommunications*, Revue internationale de police criminelle, n°464.

RICHARD Paulin (2002) *La mondialisation du marché du sexe* dans Actuel Marx 2002/1 (n°31), France.

Souheil EL ZE IN. (1998), *L'indispensable amélioration des procédures internationales pour lutter contre la criminalité liée à la nouvelle technologie*.

ZIMMERMANN Philip. (1999), *Cryptographie et réseau*, Pour la science, paris.

Webographie

http://www.bull.fr/securinews/courant/cyhack.html, *Cybercriminalité et hackers professionnels*,

https://fr.wikipedia.org. « Cheval de troie » consulté

https://WWW.avast.com. «qu'ets-ce qu'une Bombe logique ? Exemple et prévention-Avast ».

https://WWW.websecuriy.digicert.com. «Différents virus informatiques ».

https://www.enssib.fr*Criminalité Informatique*.
https://WWW.universalis.fr « Encyclopédie universalis »
https://WWW.CoursTechInfo.be. « *Historique – Les générations d'ordinateurs de 1945 à nos Jours* »
https://fr.m.wikipedia.org*Chiffrement ou cryptage.*
https://solutions.lesechos.fr PEM : *Comment se protéger du piratage Informatique*.
https://www.faronics.com.*7categories de criminels informatique.* Poster par ASMITH 3/11/2020.