Problématique de la cybercriminalité et respect de l'éthique de liberté

Dr Bouassida Khouloud / enseignante chercheuse -
Institut Supérieur des Arts et Métiers de Sfax- Université de Sfax – Tunisie

Problamatic of cybercrime and respect for the ethics of freedom

Dr Bouassida Khouloud / teacher researcher -
Higher Institute of Arts and Crafts of Sfax
- University of Sfax –Tunisia

ملخص: الجريمة السيبرانية هي نشاط إجرامي يتم تنفيذه عبر الفضاء الإلكتروني والإنترنت. نتيجة لتقدم الثورة الرقمية، تُمارس الجريمة الإلكترونية على نطاق واسع لتشمل جميع الأسس الاقتصادية والاجتماعية. الإشكالية الرئيسية في محاربة هذه الجريمة هي تحسين الأمن دون تقييد الحريات. ما هي الطرق المعتمدة لمحاربة هذه الظاهرة مع احترام أخلاقيات الحرية؟
تهدف هذه المقالة إلى دراسة مفهوم الجريمة السيبرانية وتثبيته في إطار إجرامي. لذلك يجب فتح العديد من مجالات البحث في ضمان الأمان والحريات الفردية فيما يتعلق باستخدام الإنترنت. تتطلب مكافحة الجرائم السيبرانية تنفيذ أساليب التنبؤ والتفاعل غير المحدود فيما يتعلق بالأخلاقيات القانونية.

الكلمات المفتاحية: الجريمة السيبرانية، الحرب الإلكترونية، الرقابة الاجتماعية، أخلاقيات الحرية، علم الجريمة، حقوق الإنسان

Résumé : La cybercriminalité est une activité criminelle effectuée à travers le cyberespace et par le réseau Internet. Résultant du progrès de la révolution numérique, la cybercriminalité se pratique à grande échelle afin d'englober l'ensemble des fondements économiques et sociaux. La problématique majeure est l'amélioration de la sécurité sans la restriction des libertés. Quels sont les outils pour lutter contre ce phénomène tout en respectant l'éthique de liberté ?

Cet article a pour but d'étudier la notion de cybercrime et de l'installer dans un cadre criminologique. Donc une multitude d'axes de recherche en matière de sécurité, de garantie des libertés individuelles en rapport avec l'utilisation d'Internet qui doivent être entrouverts. Combattre la

cybercriminalité demande la mise en place des méthodes de prévision et d'interaction illimitée à l'égard d'une déontologie légale.

Mots clés : Cybercrime, cyberguerre, contrôle social, éthique de liberté, criminologie, droit humain

Abstract: Cybercrime is a criminal activity carried out through cyberspace and internet network. Resulting from the progress of the digital revolution, cybercrime is practised on a large scale to encompass all economic and social foundations. The major problem is the improvement of security without the restriction of freedoms. What are the tools to combat this phenomenon while respecting the ethics of freedom?

The purpose of this article is to study the notion of cybercrime and to install it in a criminological frame work. It is therefore a multitude of research axes in terms of security, of guarantee of individual freedoms in relation to the use of the Internet that must be partially open. Combating cybercrime requires the implementation of methods of predicting and unlimited interaction with regard to legal ethics.

Keywords: Cybercrime, cyber warfare, social control, ethics of freedom, criminolgy, human rights

Introduction

Dans un monde hyperconnecté et avec la multiplication des dispositifs en réseau, la cybercriminalité devient une problématique mondiale. La définition de la notion de la cybercriminalité dépend de l'emploi et des objectifs de l'application de ce terme dans son contexte. Elle peut être définie comme l'ensemble des actions contestant aux lois, en employant les réseaux ou les systèmes d'information comme intermédiaires d'exécution d'un crime. Ses origines se repèrent essentiellement dans la numérisation de l'internet, le progrès technologique et la faiblesse des normes de sécurité. Un nombre étroit des opérations touchant la confidentialité, l´intégrité des données et des systèmes informatiques

définit l'analyse de la notion de cybercriminalité. Par ailleurs, des actes commis pour un intérêt personnel ou financier dans l'internet affectent l'identité personnelle des utilisateurs. Ces cybercrimes dévoilent des intentions qui dévisagent les preuves électroniques de ces actes dans un sens large, virtuel et artificiel. Ainsi, on peut saisir la notion de la cybercriminalité comme une activité criminelle opérée dans un cyberspace et via le réseau Internet (vol de données, chantage, prise en otage de ressources informatiques, …).En outre, les criminels utilisent des fausses identités pour réaliser des actions illégales telles que le blanchiment d'argent, la fraude, l'escroquerie ou même l'intrusion interdite dans des systèmes par des programmes douteux (virus, chevaux de Troie …).

De nos jours, la cybercriminalité présente une forme mafieuse engendrant des « transactions noires » d'informations piratées affectant la propriété intellectuelle, physique et morale des utilisateurs. Ce genre de criminalité virtuelle regroupe des cybercriminels, constituant ainsi une plateforme de réseaux internationaux bien organisés. Cette cybercriminalité se rend à la perception des informations vulnérables, en créant un nouveau champ de système de cyberguerre dans l'univers numérique.

La compréhension du processus d'accusation des nouvelles conduites de cybercriminalité permet d'accomplir des opérations à travers les réseaux informatiques. Ces problématiques variées sont réunies aux notions d'opportunité criminelle, de préjudice et de victimisation….Elles se contestent aux contraintes de l'éthique de liberté. La cybercriminalité demande des réponses appropriées tout en respectant les libertés individuelles, et au même temps un fondement de valeurs pénales adaptées. Elle sollicite aussi la mise en place des procédures efficaces pour mener des enquêtes dans l'univers numérique en respectant les libertés individuelles. L'utilisation croissante des réseaux sociaux a poussé les gouvernements à prendre des mesures règlementaires, dans le cadre du droit pénal. Des lois préparées luttant contre les cybermenaces, installent une polémique autour de l'éthique de liberté. Certains

spécialistes observent que ces lois sont soupçonnées d'être des prétextes pour faire un contrôle répressif dans l'espace numérique. Une révolution pourrait solliciter l'amélioration radicale dans l'application des lois pénales et dans la coopération internationale. Elle a pour objectif de combattre ce fléau tout en garantissant le respect des libertés individuelles.

Problématique de la recherche :

-Comment les effets néfastes de la cybercriminalité peuvent-ils nous conduire à prendre en compte tout type de risque ?

-Comment se dévoilent tels les rapports entre l'éthique de liberté et Internet au centre des enjeux de la société ?

-Quelles sont les solutions prises pour l'amélioration de la sécurité dans le monde d'Internet sans restriction des libertés individuelles ?

- Quels sont les outils appliqués pour lutter contre ce phénomène tout en respectant l'éthique de liberté ?

Méthodes de la recherche : nous adaptons dans notre article, une étude descriptive et analytique en se basant sur des données statistiques déjà réalisés et fondés sur des sources connues dans ce domaine tels que : l'étude CRPJ- GN-C3N, le bilan annuel du FBI, l'étude d'APWG…

Objectif de l'étude :

-Comprendre la nature de la cybercriminalité et toutes les opérations qui tournent autour de ce phénomène à travers le réseau Internet

-Saisir les mesures réglementaires et l'univers de la sécurité informatique prises par les gouvernements pour lutter contre ce genre de crime

-Etudier et établir la cohérence entre les lois pénales dans la coopération internationale et surtout en France comme exemple en respectant les libertés individuelles

I- La cybercriminalité : un phénomène étendu en vue de la création de nouvelles formes de crimes organisées

La cybercriminalité pose une discussion contestable dans le débat public et médiatique surtout pour les usagers de l'Internet. Ce phénomène n'est

pas donc des actions solitaires, additionnels ou même surprenantes, mais, il est désormais observé comme une menace sécuritaire capitale .Aujourd'hui, l'internet est devenu un vecteur parfait pour soutenir les opérations des cyber-délinquants. Ce fléau s'accroît à grande échelle dans cet univers numérique, afin de viser les infrastructures économiques et sociales.

Selon la définition de la commission européenne, on distingue trois formes majeures classifiant la notion de la cybercriminalité:

- Les atteintes touchant les systèmes d'informations, comme le blocage des systèmes ou le piratage des données.

- Les atteintes classiques, comme la fraude en ligne, le chantage, les escroqueries, les atteintes à la vie privée …

- Les atteintes de contenu, comme la pornopédophilie en ligne, le racisme, la manipulation des contenus illégaux…

Les origines de ces infractions sont parfois difficiles à préciser car les cybercriminels ont adopté des techniques modernes. Ces atteintes sont divisées en différents types, selon une étude française réalisée en 2017 par le Centre De Recouvrement Et Poursuites Judiciaires (CRPJ).On observe que 67,5% des infractions sont des escroqueries qui sont un mode de détournement très dominant. En deuxième lieu, on voit que 5,7% des actes commis se rapportent à l'appropriation de l'identité. Ensuite, l'abus de confiance vient en troisième lieu avec une estimation de 4,2%. Puis, on dévisage que le vol des données et des informations vient en quatrième lieu avec un pourcentage de 3,3% des actions commises. On peut conclure donc que la cybercriminalité classique est plus répandue dans le cyberspace. Ceci peut être expliqué par le fait que ces actions sont faciles à commettre afin d'atteindre des objectifs déterminés en temps court. Cependant, les menaces à la mort, les appels téléphoniques malveillants et la diffusion des images pornographiques sont moins répandues (<3%). Ces menaces n'offrent pas aux cyber-délinquants des gains garantis et des

possibilités à accéder aux informations utiles. Elles ne peuvent pas être bénéfiques pour ces attaquants de point de vue économique. Néanmoins, on remarque que les nouvelles tendances de cyberattaques comme la pédopornographie **interpellent les enquêteurs. En effet, le dark web (**Battu, 2018) **forme un lieu préféré pour le partage de contenus pornographiques en ligne. Il est destiné pour l'échange de contenus illégaux comme le commerce de la drogue ou même de la marchandise illégale. L'augmentation des chiffres des trafics illégaux sur le dark web est supportée par l'essor des cryptomonnaies (**Ordonneau, 2020) **et des blockchains** (Kim et autres, 2019). **Ce genre de trafic soutient le blanchiment d'argent et sa fuite vers des pays à l'étranger.**

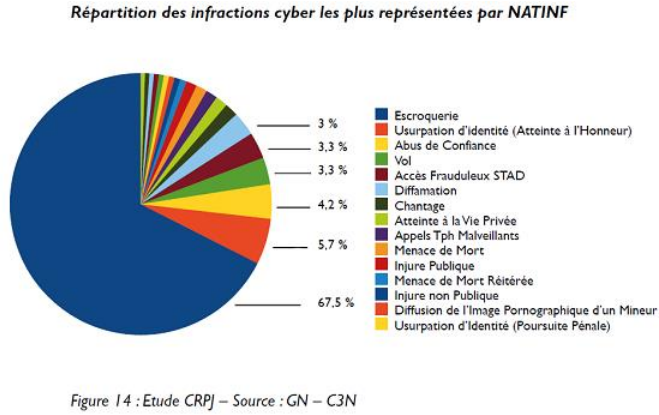

Figure 1 : répartition des cyberattaques par NATINF - Source : étude CRPJ- GN-C3N

Les technologies numériques maintiennent l'exécution d'activités délinquantes. Les cyberdélinquants emploient des moyens multiples pour arriver à leurs objectifs tout en procédant par des méthodes différentes. La cybercriminalité est un phénomène d'ordre international, car les délits peuvent être commis collectivement dans plusieurs pays. En effet, la cybercriminalité s'est répandue dans des pays comme le Brésil, la Pologne, l'Inde et la Turquie. Ces délits mettent en danger la sécurité des

internautes et des entreprises. Les Etats-Unis et la chine sont constamment les deux pays figurant à la tête de la liste, présentant le plus grand nombre des cyberattaques dans le monde. Puis viennent la France, la Russie et l'Allemagne en deuxième lieu. Ces pays présentent un taux de développement dans l'utilisation des technologies numériques, ce qui prouve cette répartition géographique distinguant les infractions dans le cyberspace (voir Figure 2).

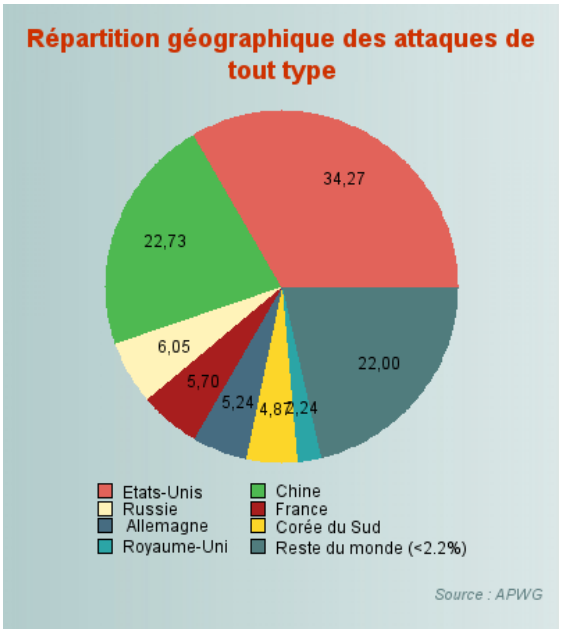

Figure 2 : répartition géographique des attaques criminelles selon les pays

Source : APWG

Selon une étude faite par la société spécialisée dans la sécurité informatique (McAfee), ce phénomène a résulté en 2008 en un préjudice d'environ 1.000 milliards de dollars. Ces dégâts sont produits par le

piratage des données informatiques des entreprises[1].L'économie américaine a déclaré un préjudice de 559,8 millions de dollars en 2009 selon le bilan annuel du FBI[2]. La France reste toujours parmi les pays les plus affectés par ce phénomène : elle se place à la 13ème place en 2009. Les cyberattaques ne prennent pas en considération les frontières et progressent d'une manière véloce. Ainsi, de nouvelles tendances de menaces virtuelles, qui entraînent des dommages graves, apparaissent. En outre, le taux de complaintes d'internautes discrédités proclamées au FBI a augmenté de 22 % en 2008.

La cybercriminalité coûte près de 600 milliards de dollars de pertes dans le monde, selon le rapport publié par le Center for Strategic and International Studies (CSIS) et par McAfee[3]. Ce rapport montre que ce coût change selon les pays et le niveau de la cybersécurité (De Fréminville, 2019). Cette sécurité est mesurée à l'aide des mesures réglementaires et du déploiement de moyens d'action. Les juristes de l'union européenne ont étudié le risque de la cybercriminalité et ses dépendances afin d'**établir une réflexion sur ce fléau. La poursuite des cybercriminels doit être suivie par une collaboration judiciaire à travers le droit pénal, garantissant le respect des libertés individuelles. Qualifier la problématique de la cybercriminalité mène directement à l'étude de la notion de la cybersécurité.** La France est d'ailleurs innovatrice dans ce domaine, grâce aux actions de l'Agence nationale de la sécurité des systèmes d'information (ANSSI)[4].

La cybercriminalité se dévoile comme étant une industrie qui menace essentiellement les entreprises à travers les vols de données et les interventions dans les réseaux. Elle se manifeste par un aspect mafieux formant de véritables « marchés noirs » parfois bien organisés. La

[1]www.mcafee.com/enterprise/fr-ca/assets/executive-summaries/es-economic-impact-cybercrime.pdf
[2]http://www.zdnet.fr/actualites/informatique/0,39040745,39750134,00.htm
[3]www.mcafee.com/enterprise/fr-ca/assets/executive-summaries/es-economic-impact-cybercrime.pdf
[4]www.ssi.gouv.fr/en/

criminalité traditionnelle et la criminalité informatique maintiennent des liens étroits. En effet, les cybercriminels utilisent des logiciels odieux pour commettre des atteintes à la propriété intellectuelle et des fraudes à la carte bancaire. La cybercriminalité traditionnelle touche l'état ainsi que les entreprises pour gagner l'argent. Ainsi, les cybercriminels procèdent à ces actes comme un métier à part entière. L'utilisation de l'Internet pour commettre des actes terroristes afin d'encourager la radicalisation et pour apprécier une sérieuse menace sur la sécurité mondiale des Etats. De plus, des réseaux de trafic élargissent leurs activités déloyales en créant des faux profils et des identités inexactes. Dans ces dernières années, on voit une nouvelle vague des menaces du Net, ce qu'on appelle « les hacktivistes » (Blampain, Palut 2000). Ces cyberdélinquants adoptent des procédés pour paralyser les réseaux des autorités dans un but politique et idéologique. Les tâches proclamées par ces Hackers sont d'ordre de cyberhacktivisme. Ici, la cybercriminalité se détourne vers la cyberguerre. En outre, la cybercriminalité est une partie intégrante, de la notion de cybersécurité. Alors, peut-on parler de la cyberprotection dans l'espace numérique ? Et à quel degré cette cybersécurité peut-elle engendrer un équilibre entre la lutte contre la cybercriminalité et le respect des libertés individuelles ?

II- Lutte contre la cybercriminalité et respect de l'éthique de liberté

1- un défi pour l'éthique de liberté

L'augmentation des actes de cybercriminalité a exigé la mise des conditions d'utilisation logique de l'Internet. Elle prescrit des répliques préventives mais aussi punitives, sans toucher les droits de l'homme. La question primordiale qui se pose est d'étudier les dispositions de lutte contre ce fléau d'une manière déontologique. La notion de l'éthique n'est pas allogène du domaine juridique, mais elle s'approche de la déontologie de lutte contre la cybercriminalité. Par exemple, l'emploi excessif des courriers électroniques et des réseaux sociaux dans les échanges des entreprises, sollicite la mise en valeur des règles éthiques. Ces règles dessinent les chartes informatiques pour prévenir les détournements

possibles. Alors, l'éthique ne se présente pas dans un contexte fixe, mais elle est applicable aux valeurs morales tout en réfléchissant sur la notion de liberté. Cette dernière dévoile un aspect intangible, tandis que, l'éthique dans son essence estime l'irrésistible de la liberté. Donc, combattre la cybercriminalité est singulièrement sensible parce qu'elle engage une normalisation de l'usage de l'Internet pouvant gêner la liberté de l'internaute.

Les investissements de la lutte contre la cybercriminalité sont généralement délicats. Il faut, alors, garantir une certaine stabilité entre le respect des libertés individuelles et la prospection des atteintes commises à travers l'Internet. Il s'agit de diminuer la profusion de la cybercriminalité en rapport du respect des règles légales. Ces règles doivent être vigilantes pour aboutir à tous les défis attendus. En outre, l'accès à l'Internet est un droit capital pour n'importe quel citoyen tout en respectant l'éthique de liberté humaine. Ainsi, les entreprises devraient prendre en compte les règles attachées à l'évolution sociale et au respect des droits. Ils doivent désigner une pratique communicative de gouvernance, accommodant les intérêts d'une approche de bonne qualité protectrice.

Le défi de la lutte contre la cyberdélinquance impose des mesures éthiques fortes. Ces mesures visent à approfondir la connaissance des judiciaires et des policiers, qui seront maniables par des règles déontologiques claires. Les Etats doivent adopter des risques à travers un système de consolidation juridique, pour collaborer entre les différents acteurs privés et publics. Les procédures sont assez sensibles et font interpeller des preuves détenues par les prestataires techniques. Ces preuves justifiant les actes de cybercriminalité, doivent répliquer aux appropriations judiciaires. Ces dernières approuvent la publication des éléments de reconnaissance des adresses IP (internet protocole).

Actuellement, les lois établies pour lutter contre les infractions engendrent automatiquement une controverse autour de l'éthique. Ces lois font un objet d'antagonisme contre cette criminologie organisée. Ce genre

de crime, on peut le considérer comme étant « un terrorisme numérique » (Vitalis, 2016). Le fondement de la conformité criminelle, doit être établi par des procédures judiciaires internationales, afin d'assurer une justice équitable. L'interprétation du code pénal sur la cybercriminalité s'installe pour instaurer une éthique de liberté citoyenne. Ces lois exigent au législateur, une requête rationnelle destinée à combattre tous les formes variées de la cybercriminalité. Bien que, pour certains, ces lois sont aperçues comme des bornes ayant pour conséquence la diabolisation de l'Internet.

Le défi est très important car il interroge la problématique de la liberté individuelle et la cybercriminalité. Il traite cette question de point de vue sociologique et législatif dans l'obligation des normes du droit. Donc, le défi est la détermination de l'éthique de liberté, dans le contenu du droit. Tandis que, le droit est d'ordre autoritaire, ne peut pas installer les valeurs de libertés individuelles dans une dimension éthique juste.

2- liberté individuelle et cybercriminalité

La liberté individuelle peut être définie comme « le droit de chacun, d'être garanti contre les arrestations arbitraires, les violations de domicile et autres attentats dont les agents de l'autorité publique pourraient se rendre coupables ; c'est le droit naturel est imprescriptible qui appartient à tout homme de disposer en pleine franchise de sa personne, d'appliquer et de développer ses facultés, non pas sous la direction, mais sous la sauvegarde de l'Etat» (Chassin, 1865). Parmi les exemples de libertés individuelles, on trouve la liberté d'expression, le droit d'accès à internet, le droit à la protection et le droit à la vie privée…

Pour saisir la notion de la liberté individuelle, on doit comprendre le mode de traitement de l'éthique de liberté et des droits législatifs liés au monde numérique. Le droit d'accès à l'internet est garanti à tous les citoyens. D'ailleurs, la liberté d'expression en ligne est protégée. En effet, la liberté individuelle forme le fondement, la prohibition et la particularité. Ainsi, le droit d'accès à l'internet résulte de cette liberté et

lui offre des options de sélection ou de filtrage des données. Les systèmes informatiques doivent être puissants face aux menaces des pirateurs. Ils doivent être équipés de nouvelles compétences à travers des analyses poussées. Ces systèmes peuvent offrir aux opérateurs des alertes de menaces contre les attaques afin de les bloquer. On peut apercevoir que certains pays développés ont adopté ce qu'on appelle le « réseau auto-protégé » (Paillard, 2011). Ce type de réseau est capable de s'instruire sur l'auto-protection face à une attaque détectée. Il peut élaborer une réponse aux problématiques de manque de compétences de lutte contre la cybercriminalité.

Dans certains pays, on observe de nouvelles lois pour lutter contre la cybercriminalité à travers des coopérations établies entre les pays. Développer la conformité des lois permet de définir la capacité d'engagement des Etats au sujet de la cybercriminalité. Poser la problématique de la cybersécurité renforce la confiance des utilisateurs d'Internet en partageant des données dans un cyberspace sécurisé. Avec le déploiement des Technologies de l'information, on observe une dématérialisation des procédures de lutte contre la cybercriminalité. En effet, la cybercriminalité est une notion polymorphe montrant des infractions nées de l'essence du système informatique. Plus le nombre de personnes connectées augmente, plus les risques de la cybercriminalité augmentent Malheureusement, les gouvernements ne mettent pas les droits de l'homme au centre des polémiques de leurs stratégies économiques et politiques. Les Etats utilisent l'excuse de la cybersécurité pour contrôler les activités des opérateurs sur l'Internet.

En conséquence, l'influence de la cybercriminalité sur la liberté individuelle est une certitude irrésistible. Sa contestation comprend une normalisation du fait, en prenant en considération le nombre croissant de victimes. Les Etats doivent innover des outils techniques efficaces tout en tenant compte des mesures de sécurité. Ces mesures doivent respecter les libertés individuelles.

III- L'effort international de prévention contre la cybercriminalité : des mesures à consolider

1- investir dans la prévention technologique

Les enquêteurs dans le domaine de la criminalité numérique ont révélé des rapports étroits entre le secteur privé et le secteur public. Ils étaient conscients par la question de la prévention et les procédures nécessaires pour lutter contre la cybercriminalité. Par exemple, l'Agence nationale de la sécurité des systèmes d'information (ANSSI), avec un budget de 100 millions d'euros participe à la création d'une stratégie politique nationale. Cette politique vise à renforcer la sécurité numérique. Elle contribue en premier lieu à la conception et à la coordination de la politique française en matière de sécurité informatique. Sa fonction primordiale vise à prévenir les infractions en aidant les opérateurs à créer des **réseaux informatiques forts.** Elle garantit des formations pour des agents compétents dans la sécurité des systèmes informatiques, Elle joue un **rôle d'exploration et d'alerte** lorsqu'une infraction est effectuée dans un tel système informatique. Ainsi, cette agence travaille sur l'identification de cette cyberattaque, afin de prendre des décisions adéquates pour la bloquer. Sa mission de **remédiation** en appliquant des mesures de sécurité urgentes, consiste à résoudre les problèmes liés aux cyberattaques dans les entreprises. A travers ses différentes missions, l'ANSSI procède à créer un environnement de confiance, de soutien et d'aide avec tous les intervenants dans le domaine informatique. En outre, les entreprises doivent contrôler leurs systèmes d'information couramment sur le plan de la sécurité. Elles peuvent profiter des services de l'ANSSI pour déterminer des règles techniques. La question de la prévention joue un rôle décisif dans la limite des cyberattaques de la part des fournisseurs de services internet. Pour évaluer les mesures de prévention en matière de cybercriminalité, les fournisseurs de services doivent contrôler leurs systèmes informatiques par de nombreux aspects techniques.

Dans l'année 2007, l'Estonie est devenue le premier pays au monde victime d'une cyberattaque à grande échelle. Cette attaque a paralysé le

gouvernement, ainsi que les systèmes informatiques. Ce qui oblige ce pays hyperconnecté à revoir ses stratégies de sécurité. La cybercriminalité n'est pas la première forme de criminalité qui sollicite des mesures juridiques globales. Pendant, ces dernières décennies, des tentatives internationales visent à prendre des défis pour déployer des accords internationaux sur cette criminalité.

2- la sensibilisation des opérateurs et des spécialistes

En adoptant une sécurité technique des réseaux contre les cyberattaques, il faut sensibiliser les chefs d'entreprises et les opérateurs. Parfois, c'est une imprudence humaine en ouvrant un fichier infecté par un virus ou un spam. Cette action mène à l'infiltration des données et des réseaux. Le groupement d'intérêt public action contre la cyber-malveillance (GIP ACYMA)[5]en France gère des actions de sensibilisation pour les opérateurs sur les menaces de cette cybercriminalité. Une étude réalisée, en 2019 par l'institut national de la consommation (INC)[6], montre que **39% des interlocuteurs indiquent qu'ils ont reçu un courrier frauduleux. 25%parmi eux étaient victimes d'un piratage de leurs comptes sur les réseaux sociaux. Cependant, 26% des victimes ont déposé une plainte.** Ceci explique, qu'il faut encore sensibiliser les gens et les encourager **pour déclarer sur toutes les menaces numériques. Le rôle de la** GIP ACYMA **et** l'ANSSI est essentiel pour donner les bons réflexes sur les risques de la cybercriminalité. A part les entreprises, les opérateurs ordinaires cherchent à acquérir des informations supplémentaires sur les modes de sécurité pour se protéger contre ces menaces.

Des formations présentées par L'ANSSI visent à sensibiliser le grand public pour se prévenir des infractions numériques. Aussi, elles posent des réflexions sur le respect de la vie privée et sur les libertés individuelles. Selon un questionnaire réalisé par des experts de l´ Office des Nations Unies contre la drogue et le crime(ONUDC) en 2013, on voit

[5] www.cybermalveillance.gouv.fr

[6]www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/top-3-menaces-cyber-2020

que les thèmes de formation sur la cybercriminalité sont diversifiés.25 % des thèmes portent sur l'étude du contexte juridique pour faire les enquêtes sur les cybermenaces. Ils visent aussi à étudier les lois et leurs modes d'application.10 % des thèmes de la formation tournent autour de la conservation des preuves pendant les enquêtes. Alors que, 5% des thèmes se concentrent sur les enquêtes avancées sur l'Internet et l'examen des téléphones mobiles pour détecter les infractions numériques. Ceci montre que les études avancées sur les cyberattaques sont très sensibles car elles touchent la vie privée des individus. De plus, les moyens techniques et technologiques restent limités pour mieux conquérir le cyberspace. Donc, les thèmes de formation destinés pour les juristes et les spécialistes restent limités. Ces formations demandent plus de renforcement sur le plan théorique, contextuel et technique.

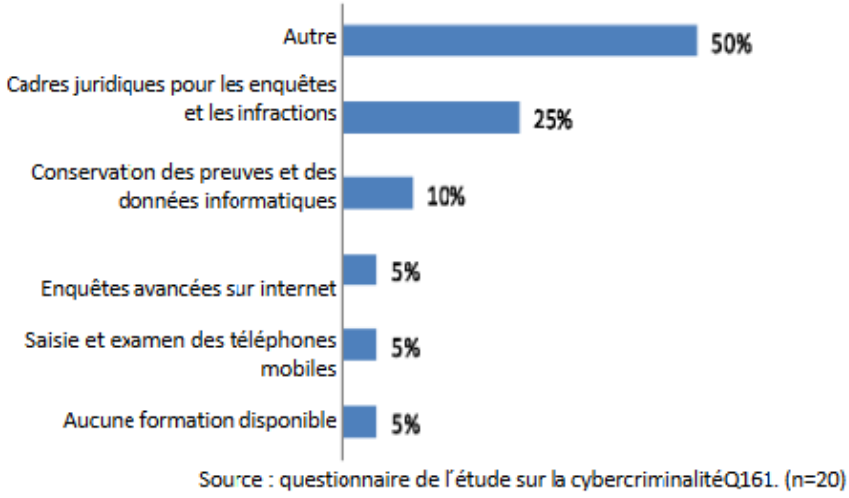

Figure 3 : Schéma montrant les thèmes de formation pour les procureurs spécialisés
Source : questionnaire de l'étude sur la cybercriminalité Q161(ONUDC), 2013

En outre, les universitaires participent notamment à la sensibilisation contre la cybercriminalité à travers les recherches et les contributions académiques. Des études dans plusieurs disciplines comme l'ingénierie des réseaux informatiques, le droit criminel et la sociologie, peuvent sensibiliser les opérateurs et les juristes. Des publications récentes discutant les cybermenaces et la cybersécurité, constituent des références pour les spécialistes. De plus, elles peuvent être des sources pour développer des solutions adéquates.

Le but des stratégies de sensibilisation établies par les organismes spécialisés, c'est de protéger les données, le stockage et le traitement des informations numériques. Dans plusieurs pays, ces données sont protégées par des lois et elles sont fixées par des protocoles. Ces dernières imposent des modes d'utilisation des données personnelles. En effet, la société britannique Comparitech a réalisé une étude en 2019, pour classer les meilleurs pays ayant une bonne stratégie contre les cyberattaques. Dans cette étude, le Japon et la France sont les deux premiers pays à la tête de la liste en matière de cybersécurité.

Les recommandations :

Nous évoquons plusieurs consignes et recommandations d'après nos observations à travers cette étude :

-Renforcer les moyens techniques, logistiques et technologiques pour sécuriser le réseau internet contres les cyberattaques

-Établir un système mondial de suivi et de coopération entre les pays pour lutter contre ce fléau

-Mise en place de mesures de confinement et de limitation des déplacements des données non sécurisés sans motifs indispensables: ce qu'on appelle la cybersécurité

-Plus de contrôle pour les mécanismes d'accès aux systèmes d'information

-Mettre des lois plus adaptés et plus strictes pour limiter ce phénoméne sans toucher les libertés individuelles

-Sensibiliser les internautes contre le phénoméne de la cybercriminalité

Conclusion

Les infractions numériques sont une réalité dans le monde virtuel. Elles provoquent de grands dommages économiques et financiers aux entreprises, aux personnes et aux Etats. L'évaluation de ces dégâts est parfois difficile (problèmes d'exhaustivité des données, le manque de détails sur la transmission des données…). Le blocage économique causé par la cybercriminalité ne permet pas aux Etats d'établir des collectes des fonds publics. Ces collectes ont pour objectif de former un budget. La faiblesse du montant du budget, présente une insuffisance financière pour combattre ce phénomène.

Dans les pays en cours de développement, on voit l'essor de l'emploi des technologies de l'information dans la vie privée et publique. Mais, les lois juridiques discutant la lutte contre la cybercriminalité ne sont pas créées sous prétexte de la mauvaise utilisation de l'Internet. Cependant, les services de lutte contre les crimes commis en ligne sont impuissants ou inefficaces. Le législateur doit réagir rapidement, avec une certaine vigilance car, les cybercriminels opèrent d'une manière plus aisée. Ils ne craignent pas les poursuites judiciaires. L'éthique de liberté suscite la réflexion sur les conditions actuelles de la gouvernance de la cybercriminalité par les Etats. Ces pays doivent intégrer un réseau de collaboration actif pour lutter contre ce fléau.

Bibliographie :

1. ANDRIEUX J.P. (2007), *Introduction historique au droit*, Vuibert, Paris

2. BATTU D. **(**2018**)**, *L'histoire et l'économie du monde accompagnées par les TIC***,** éd.ISTE, p.138

3.Bigo. D. (2005), La mondialisation de l' (in)sécurité ? Réflexions sur le champ des professionnels de la gestion des inquiétudes et analytique de la transnationalisation des processus d' (in)sécurisation, in Cultures & Conflits, n° 58, p. 55-58

4. BLAMPAIN J. PALUT L. (2000), *Résistance sur internet : utopie technologique contre logique marchande*, éd. Le Harmattan, p. 113
5. BONNET T. (2017), *la crise de la sanction face à la cybercriminalité : l'exemple du droit d'auteur,* Université Laval
6. CHASSIN C.L. (1865), *Le génie de la révolution ...: La liberté individuelle. La liberté religieuse,* p.43
7. CHAWKI M. (2009), *Combattre la cybercriminalité*, Ed. De Saint-Amans
8. DE FREMINVILLE M. (2019), *La cybersécurité et les décideurs : Sécurité des données et confiance numérique*, éd. ISTE, p.36
9. FILIOL E., RICHARD P. (2006), *Cybercriminalité : enquête sur les mafias qui envahissent le web,* Ed. Dunod
10. FREYCINET E. (2012), *La Cybercriminalité en mouvement,* Hermès Sciences Publications
11. *Garland. D. (2008), On the concept of moral panic, in Crime, Media, Culture, vol. IV, n° 1, p.3*
12. GUEYE P. (2018), *criminalité organisée, terrorisme et cybercriminalité : réponses de politiques criminelles,* Ed. L'Harmattan-Sénégal
13. HELIE-GHERNAOUTI S. (2009), *la cybercriminalité : le visible et l'invisible,* Col. Le savoir Suisse, Presses polytechniques et universitaires romandes
14. HRISTOVA-G. (2018), *le phénomène « cybercriminalité »,* Ed. Universitaires Européennes
15. KIM S., DEKA. G.C., ZHANG P. (2019), *Role of BlockchainTechnology in IoT Applications*, AcademicPress, p.11
16. MUCCHIELI L. (2001), *Violence et insécurité*, La Découverte, Paris
17. VENTRE D. (2011), *cyberattaque et cyberdéfense*, Lavoisier
18. VITALIS A. (2016), *L'incertaine révolution numérique,* éd. ISTE, p. 44
19. ORDONNEAU P. **(**2020**)**, *Le Crypto-Yuan : Une première mondiale : le «bond en avant» de la Chine pour lancer la première monnaie cryptée souveraine au monde,* éd. La Route de la Soie, p.225

20. PAILLARD C.A. (2011), *Les nouvelles guerres économiques*, éd. Ophrys, p.493