CYBERCRIMINALITE

Exposé du 3ème Groupe

Membres du groupe

- Kadiatou Dian BARRY(cheffe)
- Aissatou Kindy BALDE
- Aissatou Abobo DIALLO
- Youssouf DIALLO
- Mamadou Dara SOW
- Kadiatou Sadjo BARRY
- Abel TOUNKARA
- Abdourahamane BARRY
- Mariame SOW
- Oumar SOW
- Noel LAMAH
- Elhadj Boubacar Barry
- Abdoulaye BAH
- Hafiziou BARRY
- Thierno Mouctar BAH
- Thierno Amadou Kourahoye DIALLO

Sommaire

- Introduction
- Définition
- Types de cybercriminalités
- Causes
- Conséquence
- Signes
- solution
- Articles

Introduction

L’augmentation de l’accès à Internet dans un passé récent a créé un certain nombre de nouveaux défis juridiques. Alors que l’Internet est transnational, amorphe et difficile à définir, le nouveau paysage crée par le monde numérique a souvent confondu le droit lorsqu’il s’agit de protéger les droits fondamentaux à l’ère du numérique. Les anciennes définitions de ce qui constitue un éditeur ou un journaliste sont de plus en pl us compliquées ;surmonter l’anonymat offert par de nombreuses plateformes internet peut être une entreprise difficile, voire impossible ; et il existe de sérieuses questions sur la responsabilité des contenus partagés en ligne qui peuvent affecter d’une manière ou d’une autre plusieurs parties dans différentes juridictions.

Réglementer et légiférer sur les crimes qui se produisent sur l'Internet ou qui s'y rapportent a été une entreprise difficile pour les États et les organismes internationaux. On estime que les économies africaines ont perdu 3,5 milliards de dollars en 2017 à cause de la cybercriminalité, et l'Afrique représente 10 % du total des incidents cybernétiques mondiaux. En l'absence de cadres réglementaires et de protections adéquates, la croissance de l'accès à l'internet, du commerce électronique et du développement économique pourrait entraîner une augmentation des cas de cybercriminalité.

Qu’est-ce que la cybercriminalité?

La cybercriminalité est une activité criminelle qui cible ou utilise un ordinateur, un réseau informatique ou un appareil mis en réseau. La plupart des cybercrimes sont commis par des cybercriminels ou des pirates informatiques qui cherchent à gagner de l’argent. Cependant, il arrive que la cybercriminalité vise à endommager des ordinateurs ou des réseaux pour des raisons autres que le gain. Elles peuvent être d’ordre politique ou personnel.

Le cybercrime peut être commis par des individus ou des organisations. Certains cybercriminels sont organisés, utilisent des techniques performantes et sont techniquement très qualifiés. D’autres sont des pirates novices.

Le cybercrime implique l'un ou les deux éléments suivants

- Activité criminelle visant les ordinateurs à l'aide de virus et d'autres types de programmes malveillants.
- Activité criminelle utilisant des ordinateurs pour commettre d'autres crimes

Les différents types de cybercrimes

- Fraude par email et Internet.
- L'usurpation d'identité (lorsque des renseignements personnels sont volés et utilisés).
- Le vol de coordonnées bancaires ou de données financières.
- Le vol et la vente de données d'entreprise.
- La cyber-extorsion (exiger de l'argent pour empêcher la concrétisation d'une menace d'attaque).
- Les attaques de ransomwares (un type de cyber-extorsion).
- Le cryptojacking (lorsque des pirates extraient de la cryptomonnaie à partir de ressources qu'ils ne possèdent pas).

- Le cyber-espionnage (lorsque les pirates accèdent aux données du gouvernement ou d’entreprises).
- Perturber les systèmes d’une manière qui compromet la sécurité d’un réseau.
- Violer les droits d’auteur.
- Faire des paris illégaux.
- Vendre de façon illégales des articles en ligne.
- Solliciter, prendre ou posséder du contenu pédopornographique.

Quelques exemples de cybercrime

- Faux réseaux publics.
- Phishing.
- Vol de mots de passe.
- Usurpation d’identité
- Malware (virus destructeur)
- Cyber espionnage.
- Cyberharcèlement.

Etc…..

Est-il possible d’éviter les cybers risques?

Il est évidemment impossible de les écarter totalement. Cependant, la mise en place de certains moyens techniques associés à la sensibilisation des utilisateurs permet sans aucun doute de diminuer considérablement les risques. Les acteurs de votre entreprise, ou le particulier, peuvent ainsi apprendre à gérer une éventuelle attaque et à la contenir afin d’éviter sa propagation.

Les causes de la cybercriminalité

- Espionnage
- Vol de données
- Arrêt d'un système
- Appât du gain
- Envie de nuire

Etc...

Conséquences de la cybercriminalité dans l'entreprise

- La paralysie du système informatique de l'entreprise entrainant alors une perte d'exploitation
- Le vol et la perte de données personnelles jugées sensibles
- L'espionnage notamment industriel et scientifique
- La création de faille de sécurité dans le système informatique de l'entreprise
- Une atteinte à l'image ou la réputation de l'entreprise
- L'exposition aux risques de chantage à travers les ransomware notamment.
- Un préjudice commercial

Etc…

Conséquences de la cybercriminalité sur des individues

- Le vol ou perte de données personnelles jugées sensibles
- L’espionnage
- Une atteinte à l’image ou la réputation
- Chantages et menaces
- Peur, dépression, peut même conduire au suicide

Les signes d’une cyberattaque

- Ralentissement des postes de travail.
- Surutilisation de la bande passante
- Publicités intrusives
- Activité inhabituelle sur votre site web(fort trafic soudain, par exemple)
- Messages suspects reçu ou envoyés depuis votre boite mail sans action de votre part
- Problèmes au démarrage / à l’arrêt de vos PC
- Fichier disparus, modifiés, endommagés ou encore créés
- Creation ou descruption de comptes

- Votre PC ou parc informatique est bloqué
- B Antivirus émettant subitement de nombreuses alertes
- Mots de passe modifiés sans que vous en ayez été informé ou sans que vous l’ayez souhaité
- Connexion ou activités inhabituelles sur vos comptes

Comment se protéger du cybercrime ?

- **Garder vos logiciels et le système**

  En maintenant vos logiciels et votre système d'exploitation à jour, vous bénéficiez des derniers correctifs de sécurité pour protéger votre ordinateur

- **Utiliser un logiciel antivirus et tenez-le à jour**

  Utilise un antivirus ou une solution de sécurité Internet complète comme Kaspersky Total Security est une façon intelligente de protéger votre système contre les attaques. Le logiciel antivirus vous permet d'analyser, de détecter et de supprimer les menaces avant qu'elles ne posent problème. Disposer de cette protection vous permet de défendre votre ordinateur et vos données contre le cybercrime, ce qui vous permet d'avoir l'esprit tranquille. Maintenez votre antivirus à jour pour bénéficier du meilleur niveau de protection

- **Utiliser des mots de passes forts**

  Veuillez à utiliser des mots de passes forts que les autres ne devineront pas et ne les notez nulle part. Vous pouvez également utilisé un gestionnaire de mot de passe fiable pour générer des mots de passes forts aléatoirement afin de vous simplifier la tache.

- **N’ouvrez jamais les pièces jointes contenus dans des courriers indésirables**

  Les pièces jointes des spams sont un moyen classique d’infecter un ordinateur via une attaque de programmes malveillants et d’autres formes de cybercrimes. N’ouvrez jamais une pièce jointe envoyez par un expéditeur que vous ne connaissez pas.

- **Ne cliquez pas sur les liens contenus dans les courriers indésirable ou les sites web non fiable**

  Cliquer sur les liens contenus dans les spams, sur d'autres messages ou sur des sites web inconnus est une autre méthode via laquelle les individus deviennent la cible cybercrime. Evitez de le faire pour rester en sécurité en ligne.

- **Ne partagez jamais de renseignements personnels, sauf si l'opération est sécurisée**

  Ne partagez jamais de données personnelles au téléphone ou par email à moins d'être totalement sûr que la ligne ou l'email est sécurisé. Assurez-vous que la personne à qui vous vous adressez est bien la personne que vous connaissez

- **Contactez les entreprises directement en cas de demandes suspectes**

  Si une entreprise qui vous a appelé vous demande des informations ou des données personnelles, raccrochez. Rappelez-les en utilisant le numéro figurant sur leur site web officiel pour vous assurer que vous parlez bien à eux et non à un cybercriminel. Idéalement, utilisez un autre téléphone, car les cybercriminels peuvent garder la ligne ouverte. Alors que vous pensez avoir composé un nouveau numéro, ils peuvent faire semblant d'être la banque ou l'autre organisation à qui vous pensez vous adresser.

- **Soyez attentif aux adresses URL des sites Web que vous visitez**

  Garder un œil sur les URL sur lesquelles vous cliquez. Ont-elles l'air légitimes ? Evitez de cliquer sur des liens peu familiers ou des URL qui ressemblent à un courrier indésirable.
  Si votre produit de sécurité Internet inclut une fonctionnalité pour sécuriser les transactions en ligne, vérifiez qu'elle est activée avant d'effectuer des transactions financières en ligne.

Garder un œil sur vos relevés bancaires

Il est important de déterminer rapidement que vous avez été victime d'un cybercrime. Gardez un œil sur vos relevés bancaires et contactez votre banque pour en savoir plus sur des transactions inconnues. La banque peut enquêter pour savoir si elles sont frauduleuses.

Quelques articles

Titre 1 – Infractions contre la confidentialité, l'intégritéet la disponibil

Article 2 – Accès illégal

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'accès intentionnel et sans droit à tout ou partie d'un système informatique. Une Partie peut exiger que l'infraction soit commise en violation des mesures de sécurité, dans l'intention d'obtenir des données informatiques ou dans une autre intention délictueuse, ou soit en relation avec un système informatique connecté à un autre système informatique.

Article 3 – Interception illégale

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'interception intentionnelle et sans droit, effectuée par des moyens techniques, de données informatiques, lors de transmissions non publiques, à destination, en provenance ou à l'intérieur d'un système informatique, y compris les émissions électromagnétiques provenant d'un système informatique transportant de telles données informatiques. Une Partie peut exiger que l'infraction soit commise dans une intention délictueuse ou soit en

Article 4 – Atteinte à l'intégrité des données

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait, intentionnel et sans droit, d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques.

2 Une Partie peut se réserver le droit d'exiger que le comportement décrit au paragraphe 1 entraîne des dommages série

Article 5 – Atteinte à l'intégrité du système

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'entrave grave, intentionnelle et sans droit, au fonctionnement d'un système informatique, par l'introduction, la transmission, l'endommagement, l'effacement, la détérioration, l'altération ou la suppression de données informatiques.

Article 6 – Abus de dispositifs

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, lorsqu'elles sont commises intentionnellement et sans droit:

a la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition:

i d'un dispositif, y compris un programme informatique, principalement conçu ou adapté pour permettre la commission de l'une des infractions établies conformément aux articles 2 à 5 ci-dessus;

ii d'un mot de passe, d'un code d'accès ou de données informatiques similaires permettant d'accéder à tout ou partie d'un système informatique,

dans l'intention qu'ils soient utilisés afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5; et

b la possession d'un élément visé aux paragraphes a.i ou ii ci-dessus, dans l'intention qu'il soit utilisé afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5. Une Partie peut exiger en droit interne qu'un certain nombre de ces éléments soit détenu pour que la responsabilité pénale soit engagée.

2 Le présent article ne saurait être interprété comme imposant une responsabilité pénale lorsque la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition mentionnées au paragraphe 1 du présent article n'ont pas pour but de commettre une infraction établie conformément aux articles 2 à 5 de la présente Convention, comme dans le cas d'essai autorisé ou de protection d'un système informatique.

3 Chaque Partie peut se réserver le droit de ne pas appliquer le paragraphe 1 du présent article, à condition que cette réserve ne porte pas sur la vente, la distribution ou toute autre mise à disposition des éléments mentionnés au paragraphe 1.a.ii du présent article.

Titre 2 – Infractions informatiques

Article 7 – Falsification informatique

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'introduction, l'altération, l'effacement ou la suppression intentionnels et sans droit de données informatiques, engendrant des données non authentiques, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si elles étaient authentiques, qu'elles soient ou non directement lisibles et intelligibles. Une Partie peut exiger une intention frauduleuse ou une intention délictueuse similaire pour que la responsabilité pénale soit engagée.

Article 8 – Fraude informatique

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait intentionnel et sans droit de causer un préjudice patrimonial à autrui:

a par toute introduction, altération, effacement ou suppression de données informatiques;

b par toute forme d'atteinte au fonctionnement d'un système informatique,

dans l'intention, frauduleuse ou délictueuse, d'obtenir sans droit un bénéfice économique pour soi-même ou pour autrui.

Titre 3 – Infractions se rapportant au contenu

Article 9 – Infractions se rapportant à la pornographie enfantine

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les comportements suivants lorsqu'ils sont commis intentionnellement et sans droit:

a la production de pornographie enfantine en vue de sa diffusion par le biais d'un système informatique;

b l'offre ou la mise à disposition de pornographie enfantine par le biais d'un système informatique;

c la diffusion ou la transmission de pornographie enfantine par le biais

d'un système informatique;
d le fait de se procurer ou de procurer à autrui de la pornographie enfantine par le biais d'un système informatique;
e la possession de pornographie enfantine dans un système informatique ou un moyen de stockage de données informatiques.
2 Aux fins du paragraphe 1 ci-dessus, le terme «pornographie enfantine» comprend toute matière pornographique représentant de manière visuelle:
a un mineur se livrant à un comportement sexuellement explicite;
b une personne qui apparaît comme un mineur se livrant à un comportement sexuellement explicite;
c des images réalistes représentant un mineur se livrant à un comportement sexuellement explicite.
3 Aux fins du paragraphe 2 ci-dessus, le terme «mineur» désigne toute personne âgée de moins de 18 ans. Une Partie peut toutefois exiger une limite d'âge inférieure, qui doit être au minimum de 16 ans.
4 Une Partie peut se réserver le droit de ne pas appliquer, en tout ou en partie, les paragraphes 1, alinéas d. et e, et 2, alinéas b. et c.

Titre 4 – Infractions liées aux atteintes à la propriété intellectuelle et

Article 10 – Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les atteintes à la propriété intellectuelle, définies par la législation de ladite Partie, conformément aux obligations que celle-ci a souscrites en application de l'Acte de Paris du 24 juillet 1971 portant révision de la Convention de Berne pour la protection des œuvres littéraires et artistiques, de l'Accord sur les aspects commerciaux des droits de propriété intellectuelle et du traité de l'OMPI sur la propriété intellectuelle, à l'exception de tout droit moral conféré par ces conventions, lorsque de tels actes sont commis délibérément, à une échelle commerciale et au moyen d'un système informatique.
2 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les atteintes aux droits connexes définis par la législation de ladite Partie, conformément aux obligations que cette dernière a souscrites en

Titre 5 – Autres formes de responsabilité et de sanctions

Article 11 – Tentative et complicité

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, toute complicité lorsqu'elle est commise intentionnellement en vue de la perpétration d'une des infractions établies en application des articles 2 à 10 de la présente Convention, dans l'intention qu'une telle infraction soit commise.
2 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, toute tentative intentionnelle de commettre l'une des infractions établies en application des articles 3 à 5, 7, 8, 9.1.a et c de la présente Convention.
3 Chaque Partie peut se réserver le droit de ne pas appliquer, en tout ou en partie, le paragraphe 2 du présent article.

morale par une personne physique agissant sous son autorité.
3 Selon les principes juridiques de la Partie, la responsabilité d'une personne morale peut être pénale, civile ou administrative.
4 Cette responsabilité est établie sans préjudice de la responsabilité pénale des personnes physiques ayant commis l'infraction.

Article 13 – Sanctions et mesures

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour que les infractions pénales établies en application des articles 2 à 11 soient passibles de sanctions effectives, proportionnées et dissuasives, comprenant des peines privatives de liberté.
2 Chaque Partie veille à ce que les personnes morales tenues pour responsables en application de l'article 12 fassent l'objet de sanctions ou de mesures pénales ou non pénales effectives, proportionnées et dissuasives, comprenant des sanctions pécuniaires.