LES DEFIS DE LA CYBERCRIMINALITE : PALLIER A UN LARGE DOMAINE D'INFRACTIONS

publié le **04/02/2013**, vu **4069 fois**, Auteur : Maître HADDAD Sabine

Branche pénale de l'informatique,la cybercriminalité vise les infractions commises via les réseaux informatiques ou de communication(télécommunication, radiodiffusion, smartphones….). Elle n'est pas forcément le fait d'un seul homme, mais fait jouer de plus en plus des bandes organisées, des réseaux organisés sur un plan international,si bien que la preuve du mis en cause reste difficile. Après 40.000 nouveaux signalements en janvier, EDF a admis qu'elle avait fait les frais d'une attaque « phishing » depuis août 2012...

Branche pénale de l'informatique, la cybercriminalité ou quelles infractions peuvent être commises via les réseaux informatiques ou de communication (télécommunication, radiodiffusion, smartphones….).

Elle n'est pas forcément le fait d'un seul homme, mais fait jouer de plus en plus des bandes de réseaux réalisée sur le plan international , sa preuve reste difficile

Après 40000 nouveaux signalements en janvier, EDF a admis qu'elle avait fait les frais d'une attaque « phishing » depuis août 2012

I- Une notion largement définie

Il n'y a pas de définition universelle de la cybercriminalité n'a été admise ,si bien que chaque Etat l'a défini selon ses propres critères.

En France la notion est définie largement.

A) La cybercriminalité et les atteintes aux personnes

-Diffamation,

-Injures

-Pornographie et pédopornographie, diffusion de photos

PORNOGRAPHIE ET PEDOPORNOGRAPHIE EMANANT D'UN TIERS SUR LA TOILE ET SANCTIONS PENALES

-Incitation à la haine raciale

-Atteintes à la vie privée

-Dénigrement

-Usurpation d'identité

Je renvoie le lecteur à l'analyse de ces notions dans mon article ATTEINTES A LA PERSONNE SUR RESEAUX SOCIAUX : FONDEMENTS JURIDIQUES AUX POURSUITES...

B) La cybercriminalité et les atteintes aux biens

-Téléchargement ilégal

- Hameçonnage ou phishing: technique consistant principalement à l'envoi massif d'emails afin de récupérer les informations confidentielles des internautes telles que les numéros de cartes bancaires….

- Intrusions ou piratages des données

- Différents types d'intrusions dans le système informatiquepar le biais de programmes malveillants

Le ver: pour se propager entre ordinateurs avec des séries de codes informatiques

Le virus: pour infecter d'autres programmes

Le cheval de Troie :pour avoir un contrôle à distance de l'ordinateur infecté,

Les bombes logiques: pour détruire de façon différé.

L'attaque en déni de service: pour empêcher d'utiliser un service par saturation d'exécution de programmes

Le spam: communication électronique, expédiée en masse à des fins publicitaires ou autres,

L'adware: pour afficher des bannières publicitaires,

Le spyware: pour installe un logiciel espion et imposer régulièrement des informations statistiques sur les habitudes de l'utilisateur

-l'entrave au fonctionnement d'un système automatisé de données est réprimé par l'article **323-2 du code pénal:**

« Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75000 euros d'amende ».

- La contrefaçon (vol de propriété intellectuelle) La destruction de données,

le cybersquatting pourra être de la contrefaçon en présence d'un nom de domaine similaire ou identique à une marque.

S'ACCAPARER UN NOM DE DOMAINE POUR DETOURNER UNE MARQUE SUR INTERNET, C'EST DU CYBERSQUATTING .

-Toutes sortes d'escroqueries commises via les réseaux.

(ex aux enchères sur le net, fraude à la carte bleue , vente en ligne avec encaissement sans livraison de la marchandise…)

L'Article L 313-1 du Code Pénal définit l'escroquerie :

"le fait, soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manoeuvres frauduleuses, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers, à remettre des fonds, des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge. L'escroquerie est punie de cinq ans d'emprisonnement et de 375 000 euros d'amende".

II- Le défi majeur pour pallier à ce fléau

A) Six attitudes à avoir pour tenter de pallier à la cybercriminalité

1°- déployer une vigilance de tous les instants, et surtout une vigilance parentale aussi dans information indispensable faites aux adolescents

2°- une protection de l'ordinateur par installation d'un antivirus puissant et à jour et une barrière de protection "fire wall" pour empêcher les piratages

3°- vérrouiller certains sites peut avec des navigateurs Internet en allant (Menu "options", puis "sécurité", reconnaissable par les logos Confiance,Interdit,Codé

-fixer une liste de sites autorisés ou interdits, une liste noire.

4°- procéder au signalement de sites à contenus pornographiques, ou d'incitation à la haine raciale... en mettant en scène des mineurs, au commissariat de police ou en brigade de gendarmerie

https://www.internet-signalement.gouv.fr

DENONCER UN SITE LITIGIEUX SUR INTERNET : UNE POSSIBILITE EN CAS D'INFRACTION CONSTATEE.

5°- vérifier les informations légales du site : ex SIRET, RCS

6°- déposer plainte

B) Quelle coopération ?

1°- *La création d'un groupe de travail instauré par Manuel VALLS*

La délinquance cyberceriminelle est une « économie souterraine » comme le souligne le Ministre de l'Intérieur M.VALLS et coûte des millions d'euros et de dollars chaque année.

C'est dans ce contexte qu'il a annoncé le 29 janvier 2013, la mise en place d'un groupe de travail destiné à lutter contre cette cybercriminalité.

Il semblerait que cette nouvelle législation puisse aller dans le sens d'une responsabilité des fournisseurs d'accès et des hébergeurs accrues, et remette en cause le principe de la LCEN loi pour la Confiance dans l'Economie Numérique du 21 juin 2004 et de la directive « e-commerce « de 2000.

LOI DU 21 JUIN 2004 POUR LA CONFIANCE DANS L'ECONOMIE NUMERIQUE:APPORTS DE 1ère CIV,17 FEVRIER 2011

Ainsi d'une responsabilité a posteriori liée à l'information , une implication plus importante pourrait les concerner ?

2°- La coopération internationale

a) avec la La **convention de Budapest du Conseil de l'Europe du 23 novembre 2001**

b) avec le rôle d'iinterpol pour une meilleure coopération dans l'échange d'informations entre pays membres est essentiel. Il place un réseau d'enquêteurs spécialisés .

Demeurant à votre entière disposition pour toutes précisions en cliquant sur http://www.conseil-juridique.net/sabine-haddad/avocat-1372.htm

Sabine HADDAD

Avocat au barreau de Paris