CyberEdu A1 : Le droit des TIC et l'organisation de la cybersécurité en France

Lorsque l'on parle de cybersécurité, on doit savoir ce qu'est un Cyber-Attaque. C'est une menace numérique majeure à forte probabilité et fort impact potentiel. On peut citer comme exemple récent l'attaque du CHU de Rouen où des numéros de sécurité sociale ont été dérobés. Pour s'en protéger il existe le livre blanc de la cybersécurité qui recense les moyens applicable pour se protéger des pirates informatiques.

En France, c'est le premier ministre qui dirige la cybersécurité par le biais de tous les ministères, tous sont formés à la cybersécurité. On retrouve également : Préfecture de Police, DGA, EMA, Gendarmerie et Police Nationale.

- Le SGDSN est censé piloter la politique nationale en matière de sécurité des systèmes d'informations.
- L'ANSSI est censée vérifier l'application des mesures adoptées, elle doit conseiller les administrations en matière de sécurité, informer le public et contribuer au développement du service de confiance.

Tous les domaines présents en France sont concernés par la cybersécurité : Propriété intellectuelle, vie privée, e-commerce, liberté d'expression, … La cybersécurité dépend d'un droit non-codifié, elle dépend de tous les codes présent sur le territoire français. Elle nécessite donc un effort de veille Juridique car elle dépend de beaucoup de jurisprudence. Elle a une évolution constante et est difficile d'accès.

La lutte contre la cybercriminalité (Ensemble des actes contrevenants aux traités internationaux ou lois nationales utilisant les réseaux ou systèmes d'informations pour réaliser un délit ou les ciblant) est aujourd'hui quotidienne avec les attaques comme le "fishing" ou "hameçonnage" et des groupes comme les "Anonymous". Pour lutter on utilise une méthode appelée "Investigation numérique" ou "Forensics" en anglais (Ensemble des protocoles et mesures permettant de rechercher des éléments techniques sur un conteneur de données numériques en vue de répondre à un objectif technique en respectant une procédure de préservation de conteneur), on peut citer : HADOPI ou l'écoute téléphonique. Des lois sont également passées pour pouvoir identifier ce qui est un crime de ce qui ne l'est pas. La plus connue est la "Loi GodFrain" : Votée et adoptée le 5 Janvier 1988, elle stipule que l'accès ou le maintien frauduleux dans tout ou partie d'un système de traitement automatisé de données est puni de 2 ans de prison et 30 000€ d'amande.

- Affaire Damien Bancal : En 2009, Damien Bancal a reçu une alerte d'un internaute concernant une faille de sécurité sur un serveur. Il a alors contacté l'entreprise pour les informer et a écrit un article sur son bloc. Il a été relaxé.
- Affaire Kitetoa : Un journaliste du « Canard enchainé » à découvert une faille de sécurité sur le site de TATI (textile), après avoir prévenu beaucoup de fois l'entreprise et a écrit un article sur son site. Il a été relaxé en 2002.

Le code de propriété intellectuelle gère les affaires de cybersécurité. Il y a aussi la loi pour la confiance dans l'économie numérique (date de 2004, transpose une directive européenne qui concerne le commerce électronique mais aussi sur la protection de la vie privée quand on utilise les communications électroniques).

La Commission Nationale de l'informatique et de Libellés (CNIL) à 4 missions : Informer et Protéger, Accompagner et Conseiller, Anticiper et Innover et enfin Contrôler et sanctionner. Elle est censée protéger toute donnée à caractère personnel dans le but de protéger toute personne physique identifiée ou qui peut être identifiée grâce à ces données.