UNİVERSİTE GALATASARAY
INSTITUT DES SCIENCES SOCIALES
DEPARTEMENT DE DROİT PUBLİC

LA CRİMİNALİTE SUR İNTERNET

F.Nihan Nişancı

Directeur de recherche : Prof. Duygun Yarsuvat

Mémoire pour l'obtention du DEA en Droit Public.

Février 2005

TABLE DES MATIERES

Liste des principales abréviations

Art : Article
ART : Autorité de Régulation des Télécommunications
CA : Cour d'Assise
CdA : Cour d'Appel
CCT : Code de Commerce Turc
CNİL : Comission Nationale des İnformatiques et des Libertés
CPT : Code pénal Turc
CSA : Conseil Supérieur de l'Audiovisuel
DNS : Domain Name System
FAİ : Fournisseur d'accés à Internet
FHİ : Fournisseur d'hébergement sur İnternet
İbid : Oeuvre précité
İSPA-UK : İnternet Service Providers Association of United Kingdom
İÜHFM : İstanbul Üniversitesi Hukuk Fakültesi Mecmuası (La revue juridique de la faculté de Droit de l'Iniversité d'İstanbul.)
İWF : İnternet Watch Foundation
LPPİA : Loi portant sur la Protection de la Propriété İntellectuelle et Artistique
NCPT : Nouveau Code Pénal Turc
No : Numéro
OMPİ : Organisation mondiale de la Propriété İntellectuelle
P : Page
PTT : Poste Télégraphe Téléphone
TGİ : Tribunal De Grande İnstance
Tİ : Tribunal d'İnstance

Introduction

On peut parler de Révolution dés lors qu'une suite d'événements produit des grandes transformations dans la vie des sociétés et des individus.

Les conséquences d'une révolution se manifestent en général au sein de la communauté qui l'a réalisée.

Néanmoins il arrive aussi qu'une révolution produise des effets à l'échelle mondiale. La Révolution Française (1789) par exemple, ayant généré des changements radicaux au niveau philosophique, politique et juridique en France, n'a pas tardé propager ses effets dans le Monde.

Au vingtième siècle, nous fûmes témoins d'une Révolution semblable; avec une différence : Celle-ci entraîna de grandes transformations au niveau technologique.

Dans la seconde moitié du vingtième siècle, l'homme a été l'auteur d'un développement technologique sans précèdent.

La première grande innovation fût sans doute l'ordinateur.

Cet appareil qui servait au départ à des fins scientifiques et militaires, fût popularisé à partir des années 80 avec la mise au point des micro-ordinateurs.

La deuxième grande innovation fût l'Internet. Ce dernier fût crée par des génies scientifiques américains cherchant à réaliser une interconnexion de leur ordinateur par une simple installation de câbles et de réseaux. Ils ignoraient sans doute que leur innovation allait permettre plus tard l'interconnexion des ordinateurs à l'échelle mondiale.

Ainsi la rencontre de ces deux grandes innovations, l'ordinateur et l'Internet, fût "explosive" (!) : on parlait désormais de "Révolution Informatique".

Cette Révolution entraîna des transformations radicales dans nos vies quotidiennes, sur le plan économique et même sur le plan politique.

Les Bénéfices de cette Révolution sur notre quotidien furent nombreux.

Ce développement notoire au niveau des moyens de télécommunication permit une meilleure gestion de l'emploi du temps en ôtant l'obligation de se

déplacer pour des gestes ordinaires. Il est devenu ainsi possible à l'aide d'un micro ordinateur et d'une connexion à l'Internet de poursuivre les investissements à la bourse, d'opérer des transactions bancaires (règlements de facture, surveillance des comptes etc.), d'organiser un voyage sans aller jusqu'à l'agence de tourisme, de réserver des billets d'avions et de trains, de faire même des achats chez le supermarché du quartier (!). Le courrier électronique par sa rapidité et son coût dérisoire devint un alternatif sérieux à la poste traditionnelle. L'Internet permit aussi un épanouissement intellectuel en mettant à la disposition des intéressés toutes sortes de livre et revue électronique ("*e-book*" et "*e-magazine*"), d'articles, de mémoires et de recherches scientifiques.

Sur le plan économique, la Révolution Informatique offrit aux entreprises de toutes tailles la possibilité de faire leur publicité à des coûts dérisoires, de commercialiser leurs produits à l'étranger, d'accéder au marché mondial et d'instaurer ainsi les circonstances propices à la concurrence.

Quelques chiffres pourront donner l'ampleur de la croissance et des enjeux économiques : en 1998, sur la totalité des entreprises françaises 30% utilisaient Internet et 40% des entreprises de grande taille possédaient un site Web. La même année les prévisions de ventes en ligne pour Noël aux USA, atteignaient les 40 %.[1]

Au niveau politique, l'Internet permit aux citoyens une immixtion plus profonde dans le régime démocratique. Le système de "e-governement" à Singapour fournit un bon exemple : par l'intermédiaire du site Web du gouvernement, les citoyens poursuivent les décisions et le actes gouvernementaux, adressent leurs objections, leurs complaintes et leurs besoins aux organes public.

L'Union Européenne a poursuivi cet exemple pour renforcer la conscience de citoyenneté européenne. Elle a récemment construit un site *Web*[2] pour permettre aux citoyens des pays adhérant à l'Union de poursuivre jour à jour les travaux législatifs et les décisions prises par les organes communautaires.

La Turquie a adhéré au projet de "e-Europe" durant la réunion des Chefs d'Etats de l'Union Européenne du 15-16 juin 2002. Et dans le cadre de ce projet, des travaux semblables sous le nom de "e-Turquie" [3]sont entrepris avec la collaboration

---

[1] "Le Monde", 08 déc.1998, "Le commerce électronique s'apprête à envahir Internet" article de Michel Alberganti. www.lemonde.fr/web/recherche_breve /1,13-0,37-176778,0.html (04.12.2003)
[2] http://europa .eu.int/scadplus/scad_fr.htm.
[3] "e-Türkiye".

du ministère principal. Pour l'instant nous ne disposons pas d'un site Web gouvernemental très élaboré. Mais quelques ministères (le Ministère des Affaires İnterieurs[4], le Ministère de la Justice[5], le Ministère de la Fiscalité[6] ...), le Parlement, ainsi que quelques organisations publiques (La Sécurité Sociale[7], la Banque Centrale[8], le Conseil du Marché d'İnvestissement[9]) permettent dés maintenant de poursuivre leurs travaux.[10]

Cependant ne parler que des avantages de l'Internet nous conduira à peindre un tableau entaché d'illusions et loin de rendre compte de ce qu'il est véritablement.

En effet le doyen J.Carbonnier n'avait pas tort d'affirmer dés la fin des années 70 que "l'évolution des techniques et des moeurs donne matière à de nouvelles formes de délinquances". [11]

Alors que la Révolution İnformatique donnait aux esprits sains de nouveaux moyens d'épanouissements, les esprits malsains ont vu dans l'Internet un nouveau moyen efficace de commettre des délits. L'Internet n'a pas tardé à devenir un environnement propice aux plus viles bassesses de nos contemporains.

Ainsi le vices les plus répandus comme la fraude, les atteintes à la vie privée et aux droits découlant de la propriété intellectuelle, les attaques à la sécurité des systèmes d'informations, l'échange et la commercialisation d'images numérisées d'enfants maltraités (...) ont trouvé une place à leur aise dans l'espace virtuel devenant un lieu où se développe à l'abri d'un écran informatique une criminalité réelle, multiforme et souvent insaisissable.

---

[4] www.icisleri.gov.tr.

[5] www.adalet.gov.tr.

[6] www.maliye.gov.tr.
www.gelirler.gov.tr.

[7] www.ssk.gov.tr.

[8] www.tcmb.gov.tr.

[9] www.spk.gov.tr.

[10] www.btvizyon.com.tr/viz_dergi_dosya .phtml (08.06.2004).

[11] Jean Carbonnier, "Sociologie Juridique", PUF, 1978, p 401.
D'après Fréderic-Jerôme Pansier, Emmanuel Jez, "La criminalité sur İnternet", Paris, Que Sais je? Puf, 2001.

Notre sujet étant d'étudier les vils occasionnés par l'Internet, il convient dans un premier temps de prendre connaissance du fonctionnement spécifique et décentralisé du réseau.

Nous aborderons ensuite les principales infractions commises sur Internet.

Nous verrons dans un troisième temps les moyens de luttes au niveau nationale ainsi qu'au niveau internationale contre ces crimes.

Première Partie : Les Généralités sur İnternet

Chapitre premier : La Définition de l'Internet

L'Internet est une abréviation de l'expression anglaise "İnternational network".

La traduction de celui ci en français est "le réseau informatique international"

Afin de comprendre la structure de l'Internet; il convient de l'expliquer en deux temps : il faut d'abord définir le "réseau informatique" et voir ensuite ce que l'expression "réseau inter réseaux" signifie.

Section I : La Définition du réseau informatique

Les ordinateurs disposent de plusieurs sources sur lesquelles des informations sont enregistrées.

L'expression "réseau" est utilisée en informatique pour désigner un ensemble d'ordinateurs liés l'un à l'autre de manière à échanger les informations enregistrées dans leurs mémoires.[12]

Ainsi, dans un réseau informatique il suffit d'allumer un ordinateur pour accéder aux informations contenues dans les autres.

Section II : La définition du « réseau inter réseau »

Cette expression désigne un grand réseau qui assure une connection entre plusieurs réseaux informatiques.

L'İnternet est un système de réseaux qui relie plusieurs autres réseaux informatiques entre eux à l'aide du protocole TCP/İP.[13]

İmaginons une entreprise ayant des filiales à İstanbul et à İzmir. La connexion des réseaux informatiques de ces deux filiales formera un "réseau inter réseau".

---

[12] www.olecorre.com/?motid =952.

[13] Transport Control Protocol Over İnternet Protocol. İnfra, p.8.

En somme l'Internet peut se définir de la manière suivante ;

L'İnternet est un réseau informatique gigantesque formé de plusieurs petits réseaux informatiques liés entre eux et éparpillés dans le monde. [14]

Le Tribunal Fédéral Américain donne une définition de l'İnternet plus simple mais semblable : "L'İnternet est un réseau international composé de plusieurs ordinateurs lié entre eux"[15]

Chapitre II : Histoire de l'İnternet

Bien que son utilisation a été popularisée dans le monde durant la décennie précédente, l'Internet est né bien avant; il est le fruit de la Guerre Froide. [16]

En 1957, les Soviétiques lancèrent « *Spoutnik* », le premier satellite autour de la Terre, dont l'une des fonctions était l'espionnage militaire.

Le président Américain D.D. Eisenhower qui sentit la menace dans la sécurité nationale, ordonna au département de la Défense Américaine, la création d'une agence de recherche qui fut nommée "*Advanced Research Project Agency*" (ARPA) – l'agence du projet de recherche avancée.

L'objectif de cette organisation, réunissant les génies scientifiques les plus brillants des Etats Unis, était à l'origine, de construire le premier satellite américain. İls parvinrent à leur but dans dix huit mois.

Cette organisation se concentra ensuite sur les technologies de communication et en particulier sur les réseaux informatiques.

Leur ambition était de fonder un réseau informatique capable d'assurer la communication militaire en cas de guerre ou en cas d'attaque nucléaire éventuel.

En 1969 l'Arpanet fut créé.

Le réseau était constitué de quatre ordinateurs inter reliés : l'un , à Los Angeles (UCLA), un à Stanford (SRİ), l'un à Santa Barbara (UCSB) et le dernier à Utah à Salt Lake City.

---

[14] İnan Aslan, İnternet El Kitabı, 9.Bası, İstanbul, Sistem Yayıncılık, Eylül 2001, p.4.

[15] Volkan Sırabaşı , İnternet ve Radyo Televizyon Aracılığıyla Kişilik Haklarına Tecavüz (İnternet Rejimi), Ankara, Adalet Yayınevi, 2003, p.52.
"İnternet birbirleri ile bağlı bulunan bilgisayarlardan oluşan uluslararası ağıdır".

[16] Gregory R. Gromov " History of İnternet and WWW: the Roads and Crossroads of İnternet History" .
www.netvalley.com/intval_intr.html (04.12.2003).

En 1970 de nouveaux systèmes informatiques se lièrent à l'Arpanet : ceux des universités Harvard et MİT, et des firmes BBN et SDC.

En 1971, NASA prit sa place dans le réseau.

L'Arpanet ainsi grandissant des problèmes de communications se posèrent à partir de 1974 entre les ordinateurs de différents types et de différents débits.

Afin de résoudre ce problème, le protocole TCP/İP (« *Transmission Control Protocol over İnternet Protocol* »– le protocole de commande de transmission sur le protocole de l'Internet) fût mis au point. Ce protocole assura un réseau hétérogène, s'adapta ainsi aux ordinateurs de différents débits, et permit à un simple micro ordinateur de communiquer avec un supercalculateur.

A la fin des années 70, Arpa quitta son identité militaire se fit administrer et financer par le centre nationale de la Recherche scientifique, "*The National Science Foundation*"-NSF et se mit ainsi à la portée des génies civils.

Au début des années 80, le réseau s'agrandit encore pour rendre service à la population civile américaine.

Mais il fallut attendre la seconde moitié de cette décennie afin que les habitants des pays développés appréhendent l'utilisation de l'Internet.

En 1990, Arpanet disparut au profit de la « *NSFnet* ». En 1991, pour remédier au fonctionnement peu convivial de l'Internet utilisé jusqu'alors par des génies scientifiques , le concept de « *WWW- World Wide Web* » fut mis en place par Tim Berners Lee, un employé du CERN (Centre Européenne de la Recherche Nucléaire)[17]

En Turquie, les recherches sur Internet débuta aussi en 1990 et furent mené par ODTÜ et TÜBİTAK.

Le groupe de projet fut nommé TR-NET . La première connexion fût réalisée entre ODTÜ et Washington au mois d'avril 1993.

A la fin de l'année 2001, on estimait le nombre d'internautes[18] actifs (de personnes disposant d'un ordinateur et ayant conclut un contrat d'accès a Internet

[17] Dufresne, Jacques " Histoire d'İnternet" http://agora.qc.ca/rech_int.html (27.05.2004).
[18] C'est une expression française désignant les personnes utilisant İnternet. www.olecorre.com/?motid=1552.

avec un fournisseur d'accès) a deux millions et d'internautes passifs a quatre millions.[19]

Chapitre III : Les principales notions à propos de l'İnternet

Plus qu'en tout autre domaine, la confrontation du droit et de l'Internet s'inscrit nécessairement dans la prise en considération de données techniques derrière lesquelles il conviendra de décrypter la volonté et le processus criminel suivi par l'auteur d'une infraction en ligne.

Voici les piliers fondateurs de ce grand réseau informatique :

Section I : Le protocole TCP/İP

Nous avions déjà évoqué que les ordinateurs se situant sur le grand réseau qu'est l'Internet, ne sont pas tous du même type ni du même débit.

Cela pouvait former un immense obstacle au fonctionnement du réseau si le protocole TCP/İP n'était pas mis au point. Ces protocoles sont sans doute la clé du succès de l'internet. Ce protocole a permis d'installer un langage unique entre les ordinateurs de structure différente et a assuré ainsi leur communication selon le mode serveur /client.[20]

TCP/İP désigne les deux protocoles principaux qui sont le support de l'Internet : TCP et İP.

Sur l'Internet la circulation d'information se fait par l'intermédiaire des paquets : cette expression vient de l'anglais "*packet*" et désigne un certain nombre d'octets (caractères ou données) transitant ensemble sur le réseau İnternet. Une communication est généralement composée de plusieurs paquets qui voyagent indépendamment sur le réseau et sont regroupés au point d'arrivée. L'acheminement de ces paquets d'informations d'un ordinateur à l'autre ou d'un réseau à l'autre se fait à l'aide d'un ordinateur consacré à cette fonction: le routeur (de l'anglais

---

[19] İnan, op.cit, p.4.

[20] Tan Deniz Sarıhan, Herkes için İnternet, İstanbul Desnet Yayınları 1998, s.32.

« *router* »). Les routeurs se relaient les paquets jusqu'a ce que ceux ci atteignent leur destination.[21]

Bref, le protocole İnternet (İP) est le protocole de communication qui régit la circulation des paquets d'informations dans le réseau İnternet.

Le TCP[22] est le protocole d'interconnexions de réseaux dont la fonction est de maintenir la connection logique de bout en bout et assurer la fragmentation et le réassemblage des paquets fournis depuis les autres couches vers leurs destinations.

Section II : L'adresse İP

Toute machine connectée à l'Internet (ou un réseau privé utilisant le protocole TCP/İP) possède une adresse İP, constituée d'une suite de chiffres qui marque sa localisation sur le réseau et qui permet de l'identifier de façon unique. [23]

Une adresse İP est constitué de quatre groupes possédant chacun trois chiffres. (par exemple 111.222.333.444[24]) cette adresse est parfois traduite en lettre compréhensible (« www.gsu.edu.tr » par exemple) grâce au système DNS[25]. C'est ainsi que se détermine la location sur İnternet d'un document son URL.[26]

---

[21] http://www.cjl.qc.ca/iabdd/iabdd2000/glossaire.htm (12.06.2004).

[22] www.zapilou.net/index.php?typ=1&key0tcp (12.06.2004).

[23] Sarıhan, op.cit, p 33.

[24] İl s'agit ici d'un protocole Internet version 4. L'adresse İP est codée sur 32 bits usuellement écrits sous formes de 4 chiffres décimaux séparés par des points. Le protocole İPv4 est la version actuelle qui arrive à sa saturation. Elle devrait prochainement être remplacé par İPversion6. Dans ce cas, l'adresse sera codée sur 128 bits qui seront écrits sous la forme ffff.ffff.ffff.ffff.ffff.ffff.ffff.ffff. İPv6 permettra un nombre énorme d'adresse : environ 6000 milliards par m2 de surface terrestre.
D'après www.zapilou.net/index.php?typ=1&key=ipv4 (12.06.2004) et www.zapilou.net/index.php?typ=1&key=ipv6 (12.06.2004).

[25] Domain Name System : Le DNS est un service disponible sur le réseau İnternet permettant de traduire les adresses textes ou URL saisie par l'utilisateur en une adresse İP. Ce service permet de mémoriser l'adresse d'un site sous la forme « www.monserveur.com » plutôt que d'avoir à se souvenir de son adresse İP (par ex.111.222.333.444)
Définition retirée de « www.geocities.com/paris/5587/dico.html » « *the French Net Dictionnary* » 7/11/2002).

[26] « *Uniform Ressource Locator*» :
C'est le mécanisme qui fournit une convention unique de noms pour tous les points du Web.
D'après www.olecorre.com/?motid=788.

Section III : Le navigateur[27]

C'est le logiciel informatique qui permet de visualiser les pages Web et de naviguer dans la hiérarchie des documents. Les logiciels essentiels sont le « *Netscape Navigator* », « *Microsoft İnternet Explorer* » et le « *Spy Mosaic* ».

Section IV : Le "*World Wide Web*"

"La Toile d'Araignée Mondiale", fruit du travail d'un groupe de personnes qui cherchaient à exploiter les possibilités de réseaux existants afin d'y faire circuler des contenus multimédias, est le service le plus connu de l'İnternet puisque toute adresse URL débute obligatoirement par « http://www. »[28]

Le "WWW" est l'ensemble des sites Internet accessibles en général via le protocole HTTP[29], constitué de bases de données et de fichiers accessibles via un navigateur situé sur l'ordinateur de l'internaute.[30]

Ces sites Internet répartis structurellement et géographiquement, sont constitués de textes, d'images et parfois de sons ou de vidéos, le tout étant reliés par des liens hypertextes internes (liens vers d'autres pages a l'intérieur du même site), ou externes (liens vers un autre site).[31]

---

[27] "*Web browser*" en Anglais .

[28] Asha Kalbag , Dünyayı saran Ağ: www, 5.bası, Ankara, Tübitak Yayınları, 2000, p.5.

[29] "http" est le protocole qui permet le transfert de page HTML (langage utilisé pour créer des documents a destination du Web) entre un serveur et un client.
D'apres www.zapilou.net/index.php?typ=5&key=000071 (12.06.2004).

[30] www.zapilou.net/index.php?typ=5&key00217 (12/06/2004).

[31] Kalbag, op. Cit, p 6.

Chapitre IV : Les principales utilisations de l'Internet

Voici les principales utilisations de l'Internet connaissant toutes des problèmes de criminalité aujourd'hui.

Section I : Le Courrier électronique[32]

C'est le service de l'Internet le plus utilisé. Le courrier électronique est le système de courrier digital sans papier.

Ce système fonctionne sur le principe de boite à lettres et correspond à la location d'espace sur le disque dur d'un ordinateur lié au réseau.

Afin d'utiliser le service de courrier électronique, les internautes doivent disposer d'une adresse e-mail sur internet. L'apparence générale de celle ci est ainsi:

« Le nom de l'internaute @ le nom de domaine. Suffixe. Lettres déterminant pays d'origine. »

Le nom de l'internaute sert à identifier la boite sur le serveur de courrier.

Le nom de domaine est en même temps le nom du fournisseur d'accès. Tous les services de courriers ont un nom de domaine unique qui les distingue des autres. C'est ce qui permet à tous les utilisateurs d'Internet d'avoir une adresse unique au monde. Les internautes n'ont pas de contrôle sur cette partie de l'adresse à moins qu'ils aient eux même un nom de domaine.

Le suffixe sert à classer les organismes selon leur champ d'activités.

Enfin les deux dernières lettres servent à déterminer le pays d'origine.

Le courrier électronique est conçu de manière à transmettre les messages le plus rapidement possible et pour cela les informations transitent en paquets d'un réseau informatique à l'autre, d'un ordinateur à l'autre. Ainsi les messages sont de nombreuses fois reproduits sur de différents disques durs pour pouvoir arriver jusqu'à son destinataire; ce qui augmente les risques d'interception. C'est la raison pour laquelle les risques dérivant de l' « *e-mail* » sont nombreux, surtout sur le plan de la vie privée.

---

[32] "*electronic mail*" en anglais soit "*e-mail*".

Le courrier électronique pose également des problèmes quand à la détermination de l'identité de son propriétaire, lorsqu'il s'agit d'un service gratuit disponible par le biais du web. (Les services « *Hotmail* », « *Yahoo* »...)[33].

Section II : L' « *İRC* » ou messagerie instantanée

L' « *İRC* » (« *İnternet Relay Chat* ») est le protocole permettant la communication directe entre deux personnes connectées simultanément à l'İnternet.

C'est un mode de communication supporté par logiciel permettant d'échanger en temps réel avec d'autres personnes, peu importe où elles se trouvent pour autant qu'elles soient reliées par ce mode.

Son appellation populaire est le "clavardage" "ou "*chat*" en anglais.

Même s'il existe de différents serveurs « *İRC* » sur Internet : « *mİRC* », « *İCQ* » (....), tous permettent ce type de lien. Une fois la connection établie avec un de ces serveurs, on accède à un environnement appelé "chambre virtuelle" ou canal. On se retrouve alors en liaison avec une ou plusieurs personnes à la fois qui peuvent lire ce que l'on inscrit au clavier de l'ordinateur.

Ces canaux, aussi nombreux que variés, sont très volatiles : si tous les usagers quittent une chambre virtuelle, elle se referme et n'existe plus.

Ce service du net aussi pose beaucoup de problèmes juridiques. Les réseaux pédophiles, satanistes pirates (..) discutent par son intermédiaire. La répression des crimes qu'ils commettent dés lors devient difficile en raison du manque de preuve : les crimes passent le plus souvent inaperçus car il n'est pas toujours possible de surveiller le contenu des canaux de discussion.

Section III : Les forums de discussion et Usenet

L' « *Usenet* » est un tableau d'affichage électronique et regroupe tous les messages reçus par sujets.

A l'aide d'un logiciel spécialisé[34] on peut dés lors échanger diverses opinions sur un domaine particulier.

---

[33] Dans ce cas, l'internaute n'est pas obliger de révéler sa vrai identité pour s'attribuer une boite et adresse e-mail.

[34] " *Microsoft Outlook Express*" par exemple.

On dit que les forums de discussion sont un mixage du clavardage et du courrier électronique, avec quelques différences cependant…

La différence entre l' « *IRC* » et les forums est la suivante : les conversations ne se font pas de manière instantanée. Et contrairement au courrier électronique où les discussions se font en privé, dans « *Usenet* » tous ceux branchés à Internet ont accès à l'intérieur du forum où les discussions se font en public.

On distingue deux sortes de forums de discussions : les modérés et les non modérés.

Les forums de discussions "modérés" disposent d'un modérateur qui émet les sujets de conversations et oriente par la suite les discussions. Ce particulier a également le droit d'effacer les messages hors sujets.

Dans les forums non modérés, il n'existe pas de contrôle à priori des messages.

Section IV : Le transfert de dossiers.

Le transfert de dossiers se fait à l'aide du "*File Transfert Protocol*".

Le « *FTP* » est un autre protocole de communication qui permet le téléchargement c'est à dire, la copie par l'utilisateur d'un fichier situé sur le serveur.[35]

Le protocole « *FTP* » a pour objectifs de permettre un partage de fichiers entre machines distantes, de permettre une indépendance aux systèmes de fichiers des machines clientes et serveuses, et de permettre de transférer des données de manière efficace.[36]

Ce protocole est le plus souvent utilisé sans même se rendre compte à l'aide du courrier électronique ou du navigateur, lorsque le téléchargement d'un fichier sonore ou d'une image est commandé.

Il est à noter que c'est par cette voie que les programmes piratés se diffusent.

---

[35] On peut retrouver sur les serveurs "*FTP*" d'énormes librairies de sons, d'images ou de logiciels de domaine public de toutes sortes. La plupart des compagnies ont aussi un serveur "*FTP*" pour permettre de venir récupérer les documents, logiciels ou informations diverses qui ont trait a l'entreprise.

[36] www.commentcamarche.net/internet/ftp.php3 (15.06.2004).

Section V : Le Telnet

Le Telnet est un protocole de communication qui permet d'effectuer une prise de contrôle a distance sur un ordinateur connecté au réseau[37].

Il permet d'établir une connection d'un ordinateur à l'autre et mettre en marche les programmes enregistrés sur l'ordinateur connecté.

Le Telnet est l'instrument privilégié des bibliothèques : les bibliothèques informatisées stockent les données bibliographiques sur un ordinateur central. Les étudiants désirant connaître la disponibilité d'un livre n'ont qu'à s'installer devant un terminal et demander à l'ordinateur central d'effectuer la recherche. Le lien qui unit ces ordinateurs et qui permet l'accès au serveur est assumé par Telnet.

Cependant ce système connaît des risques : le Telnet n'a pas pris beaucoup de temps pour devenir le moyen privilégié des intrusions illicites dans les systèmes informatiques.

Chapitre V : Les acteurs de l'internet.

Section I : Les Fournisseurs d'Infrastructure

Les fournisseurs d'infrastructure sont les sociétés de télécommunication et les câblodistributeurs qui permettent le transport "matériel" des informations sur le réseau. Ils sont donc des intervenants purement techniques[38].

Section II : Le Serveur

Le serveur désigne en général un ordinateur assez puissant et muni d'une quantité importante de mémoire et de capacité de stockage suffisante qui assure des fonctions communes pour un groupe d'utilisateurs plus ou moins important. Un serveur est en général en fonctionnement 24h/24, et peut héberger plusieurs centaines de sites Internet et être utilisé simultanément par des milliers d'internautes.[39]

---

[37] www.net-dico.com/termes/t.html (15.06.2004).

[38] www.juriscom.net/pro/1/resp19990121.htm (15.06.2004).

[39] www.zapilou.net/index.Php?typ=5&key=001601 (15.06.2004).

Section III : Les Fournisseurs d'Accès à İnternet [40]

Les fournisseurs d'accès sont les sociétés regroupant les solutions permettant l'accès du public à l'İnternet au travers différents types de connections.[41]

"C'est le sujet qui tient dans sa main la clé de la porte de l'İnternet" dit-on.[42]

Les fournisseurs d'accès sont généralement des entreprises commerciales. Mais il arrive aussi que certains établissements académiques assurent à leurs enseignants et étudiants une connection à İnternet. İls endossent dans ce cas les mêmes fonctions et responsabilités que les fournisseurs d'accès.

En Turquie, il n'y a aucune dispositions légales les concernant. On les considère comme des entreprises commerciales au sens de l'article 12 du Code De Commerce Turc. Leur fondement se fait alors en observant les conditions inscrites dans ce code.

Les services des FAİ en Turquie sont généralement offerts par abonnement.

L'offre d'un nom d'utilisateur, d'un code secret, et d'une adresse "e-Mail" est généralement inclus dans leur service.

Section IV : Les Fournisseurs d'Hébergement [43]

Les fournisseurs d'hébergement sont des sociétés regroupant des services d'hébergement sur İnternet. Un hébergement correspond en principe à la location d'un espace disque de taille variable accompagné de divers scripts, statistiques, sauvegarde (...) sur un serveur connecté en permanence à l'İnternet. Le fournisseur

---

[40] Les Exemples de FAİ en Turquie
Les entreprises commerciales : Superonline,Tr-net, Turknet (...)
Les établissements académiques : ODTÜ, İTÜ
Les établissements publics : TÜBİTAK
İl ya actuellement pres de 100 établissements qui exercent les activités de FAİ.

[41] www.zapilou.net/index.php?typ=5&key=000052.

[42] "İnternet ve Hukuk" www.superonline.com/hukuk/hukuk.htm (23.12.2003).

[43] www.zapilou.net/index.php?typ=5&key=000056 (15.06.2004).

d'hébergement doit garantir que son serveur sera accessible par les internautes de façon permanente et fiable et doit offrir une bande passante de connexion suffisante.

L'hébergeur agit donc comme un bailleur : İl loue un emplacement sur le Web ou le locataire pourra publier ce qu'il veut.

Ces fournisseurs offrent souvent des services d'hébergement mais permettent rarement d'avoir son propre nom de domaine.

L'hébergement est souvent considéré comme un métier spécialisé car les serveurs et les systèmes de routage nécessitent des personnels très qualifiés, des installations très pointues (salles protégées, climatisé, alimentations électriques sans coupures etc.) Une société peut être son propre fournisseur d'hébergement et fournisseur d'accès mais cela nécessite des moyens humains et techniques importants.

Section V : L'Hôte.[44]

C'est un ordinateur sur le réseau TCP/İP qui héberge une ressource consultable à distance par un client à travers l'İnternet.

Un fournisseur d'hébergement peut servir d'hôte en conservant dans son ordinateur des informations appartenant à l'un de ses clients et faisant en sorte qu'elles soient accessibles par İnternet.

Section VI : Les Webmestres ou les fournisseurs de contenu[45]

Le webmestre est la personne chargée de la maintenance et du suivi d'un serveur ou d'un site de la toile du Web.

Les webmestres sont ceux qui créent un site WEB et préparent des informations pouvant être accessible par l'intermédiaire d'un téléchargement.[46]

Les webmestres sont les sujets "*sine qua non*" du cyberespace : sans eux, ce dernier ne pouvait exister.

---

[44] "*Host*" en Anglais.

[45] "*Webmaster*" en Anglais.

[46] Asha Kalbag, , Bilgisayar'daki adresiniz Web sitesi,5.bası, Ankara, Tübitak Yayınları, 2000, p.4 .

Section VII : Le modérateur Usenet

L'Usenet est constitué de plusieurs groupes d'informations et de discussions. La plupart de ces groupes sont modérées, c'est à dire gérée par une personne qui reçoit et publie les messages envoyés. Les messages sont triés selon qu'ils sont conformes ou pas au but du groupe de discussions. Cette personne est donc responsable du serveur auquel le groupe d'information est attaché. Les messages ne présentant aucun lien avec le but du groupe ou ceux qui sont constitutifs de délits sont automatiquement éliminés.

Dans les groupes d'informations non modérés un tel contrôle ne peut avoir lieu.

Section VIII : L'internaute

L'internaute est l'utilisateur de l'Internet en général et plus particulièrement du Web.

Deuxième Partie : Les comportements criminels sur Internet

Chapitre Premier : Aspect juridique de l'İnternet et son lien avec la liberté de pensée, d'expression et de communication.

L'İnternet n'est pas un support de Média au sens classique.

Sa caractéristique principale est l'absence de propriétaire. Ni techniquement, ni juridiquement, l'Internet n'est assujetti à la propriété de quiconque.

Son architecture est distribué et non hiérarchique. İl fédère une multitude de réseaux différents quand à leur nature, origine, fonctionnement. Les ordinateurs qui y sont connectés appartiennent indifféremment à des établissements publics, des organismes privés à but lucratif ou non, ou à des particuliers. Le "réseau des réseaux" n'appartient donc à personne et connaît une gestion totalement décentralisée.

Les İnternautes sont les propriétaires du Web et assure la gestion de l'İnternet tous ensemble : aujourd'hui, un outil de création de site Web permet virtuellement à n'importe quelle personne qui a accès à l'Internet de poster un site Web et de contribuer a sa définition.

Selon le créateur du WWW Tim Berners Lee, le but de l'Internet est le suivant : "Le rêve au delà du Web est un espace d'information commun dans lequel nous communiquerons le partage d'informations."[47]

La conséquence majeure de cette structure de l'İnternet est que les internautes n'ont besoin d'aucune autorisation légale pour accéder à l'İnternet et bénéficier de ses services.

Le fait que l'Internet ne disposent pas d'un mécanisme de gestion centralisé présente certains avantages ainsi que des désavantages :

Les faits que le fonctionnement de l'İnternet ne soit dépendant d'aucun organisme et que les internautes n'ont besoin d'aucun accord pour accéder à l'Internet sont les avantages.

Le désavantage est le manque d'une autorité qui puisse surveiller et poursuivre les utilisations malveillantes du Web.

---

[47] www.chez.com/histoireinternet/internet_suite.htm (11.04.2004).

Le caractère décentralisé de l'Internet et son manque de propriétaire offrent l'occasion favorable au développement de la liberté d'expression et communication, composant « *sine qua non* » des sociétés démocratiques.

De nos jours le moyen le plus efficace, de faire circuler ses idées est les supports médiatiques car ceux ci s'adressent à des masses.

Ses caractéristiques font de l'Internet un support excellent à l'exercice des libertés d'expression et de communication.

De plus l'absence d'autorisation légale pour accéder à Internet est un autre atout pour l'exercice de ces libertés.

Cependant, l'exercice malveillant de la liberté d'Expression et de communication et le manque d'une autorité qui puisse sanctionner les utilisations de mauvaise foi ont très vite donné naissance aux dérives sur l'Internet.

C'est ce que l'on va voir dans le chapitre suivant.

Chapitre II : La nature des comportements criminels sur Internet

Section I : La qualification juridique des cybercrimes

Sous Section I : La définition du "cybercrime".

Afin de définir le cyber crime nous devons d'abord aborder la notion de "cyber espace".

Le terme de "cyber espace" a été utilisé pour la première fois par le romancier William Gibson, dans son roman de science fiction "*Neuromancer*" pour désigner "un environnement virtuel n'ayant pas d'existence réel dans lequel la communication électronique s'établit. Cet environnement est représenté comme l'intérieur d'un système informatique"[48]

---

[48] Yaman Akdeniz– Clive Walker – David Wall , The Internet Law and Society, United Kingdom - Essex, Longman Pearson Education, 2000, p.3.

Le cyber espace signifiait dans le roman un environnement qui échappait au contrôle des gouvernements et des Etats.

Cette expression ne faisait pas référence à la notion de liberté mais au manque de contrôle ou de censure.

Les termes d'Internet et de cyber espace sont souvent utilisés comme des synonymes, mais ne le sont pas.

Le terme de cyber espace recouvre les notions d'İnternet et ainsi que d'İntranet.

L'İntranet est le réseau informatique interne autogéré qui relie plusieurs utilisateurs au moyen de l'Internet, en général à l'intérieur d'une organisation[49]. İl est utilisé en général pour améliorer l'accès à l'information et le transfert de données entre les utilisateurs individuels et l'organisation. Grâce au protocole TCP/İP, un protocole peut se transformer d'un simple site Web contenant le livre des employés sous le format HTML à un centre de communication.

Avec ses particularités l'intranet peut être comparé à l'Internet réduit à l'échelle d'une entreprise.[50]

Le cyber espace étant une notion englobant l'intranet et l'İnternet, les crimes commis sur intranet seront qualifiés de cybercrimes mais ne pourront être qualifiés de crimes d'İnternet.

Tous les crimes commis sur İnternet sont des cybercrimes mais tous les crimes commis sur le cyber espace ne sont pas crimes d'internet.

Mais il est à noter toutefois que l'utilisation du terme «cybercrime » pour désigner l'ensemble des crimes commis sur İnternet est très courante dans la pratique. Nous utiliserons aussi cette dénomination, afin de ne pas trop s'écarter des pratiques de la vie quotidienne.

Face à l'augmentation de la délinquance dans le cyber espace, les autorités judiciaires doivent réagir pour mettre en place un système de répression correct, c'est à dire concordant avec les caractéristiques de l'Internet et assez dissuasif. Pour adopter des mesures à la hauteur de ces ambitions, il est nécessaire de qualifier la nature des cybercrimes à et de bien cerner leurs particularités.

---

[49] Sarıhan, op. Cit, p.44 .
[50] İbid, p.44.

Dans la recherche d'un système de répression efficace, deux théories sur la nature des crimes commis sur İnternet ont été mises au point par des juristes américains.[51]

La finalité de ces deux théories a été de répondre aux questions suivantes : quel type de crime est commis sur İnternet ? Est ce que l'İnternet a donné naissance à des actes illicites aux résultats dommageables auparavant inconnus par la communauté ?

La première théorie prétend que tous les crimes commis sur İnternet sont des crimes conventionnels et que l'İnternet ne sert que de support à leur réalisation.

La deuxième prétend identifier l'existence de comportements criminels spécifiques à İnternet, présentant donc un caractère « *sui generis* ».

Sous section II : Les Théories sur la qualification du cybercrime.

A. Les Cybercrimes : une nouvelle forme des crimes conventionnels[52]

La première des théories affirme que tous les comportements délictueux observés sur Internet sont une manifestation des crimes conventionnels, préalablement codifiés.

Les cybercrimes sont selon cette théorie une autre forme des crimes du monde réel. Leur différence est le monde dans lequel ils sont commis. Les crimes conventionnels commis dans le monde réel possèdent une réalité physique saisissable par nous tous, alors que les cybercrimes sont commis dans le cyberespace, c'est à dire dans un environnement d'une vérité conceptuelle mais n'ayant aucune réalité physique. L'İnternet ne sert que d'un simple support à la réalisation des crimes conventionnels. C'est la raison pour laquelle un régime juridique pénal spécifique aux cybercrimes n'est pas requis, car cette seule différence ne peut empêcher les règles générales du droit pénal de s'appliquer dans le cyber espace.

---

[51] İl n'est pas surprenant que les premières théories se rapportant à ce sujet aient été élaborées par des Américains. En effet, l'İnternet est né aux Etats Unis et la banalisation de son utilisation s'est réalisé en premier dans ce pays. Par conséquent, les dérives découlant de l'utilisation de l'İnternet ont apparu en premier là ba, ce qui a poussé les juristes à produire des solutions.

[52] Susan W.Brenner, "İs There Such a Thing as Virtual Crime?" http://boalt.org/CCLR/v4/v4brenner.htm (06.12.2003).

Pour démontrer leur constat, les partisans de cette théorie procèdent à une analyse comparative des éléments constitutifs des cybercrimes les plus commis avec ceux des crimes conventionnels.

Ils pensent que si des différences existent entre ces deux catégories de crimes, elles doivent se manifester dans leurs éléments constitutifs respectifs. Au cas où aucune différence ne pourra être constatée la crédibilité de leur théorie sera justifiée.

Les éléments constitutifs en question sont l'élément matériel, l'élément moral et l'élément d'illégalité. Il est à noter que les pères de cette théorie sont d'origine californienne. Les exemples que nous citerons ci-dessous proviendront la Loi Pénale de l'Etat de Californie.

a) Délit de vol et de détournement d'une somme.

Le délit de vol est généralement défini en Droit américain, comme l'appropriation illégale d'un objet mobilier appartenant à autrui, dans l'intention de le dépourvoir de sa propriété.[53]

Les éléments constituants de ce délit sont :

Le fait pour l'auteur du crime de s'approprier un objet mobilier appartenant à autrui constitue la conduite de l'élément matériel.

Et le fait pour le propriétaire de l'objet qu'il soit dépourvu de sa propriété, est le résultat de la conduite.

L'élément moral du crime est l'intention de dépourvoir quelqu'un de sa propriété.

Enfin, l'élément d'illégalité est le fait que l'auteur du crime n'ait pas un droit légitime pour agir ainsi.

Le délit de vol en tant que cyber crime comprend le vol d'information, de service, d'argent ou d'autre propriété.[54]

Ainsi pour les partisans de cette théorie, le délit de vol conventionnel et les alternatives sus cités sont indistincts à un ou deux éléments près.

Les mêmes éléments constituants peuvent être utilisés pour imposer la responsabilité à l'auteur du cyber crime de vol.

Prenons l'exemple le plus courant : quelqu'un utilise l'ordinateur pour pénétrer le système informatique d'une institution financière et accomplit un transfert

[53] ibid, p.6.
[54] ibid, p.9.

de fond, du compte de cette institution à son propre compte « *off shore* ». Dans ce cas, l'auteur s'est approprié illégalement de l'argent d'autrui et la victime a ainsi été dépourvue de sa propriété.

La seule différence entre le délit de vol dans le cyber espace et celui commis dans le monde réel est le moyen utilisé pour commettre le crime : dans le premier cas, l'auteur de l'acte se sert de l'ordinateur pour arriver à ses fins, alors que dans le second il fournit des efforts physiques.

En dehors du moyen utilisé, les éléments constituants du crime demeurent les mêmes. Le crime de vol dans le cyber espace ne présente donc aucune originalité par rapport au crime de vol traditionnel.

Les mêmes propos sont valables pour le vol de service et le vol de logiciel informatique.

b) La fraude

Le délit de fraude consiste dans le Droit américain[55] en la réalisation consciente de la représentation fausse d'une réalité matérielle dans l'intention de faire tomber la victime dans l'erreur et de la dissuader de transférer sa propriété à l'auteur du crime.

Les éléments constituants de ce crime sont :

Le fait de faire tomber une personne dans l'erreur par la représentation fausse d'une réalité matérielle constitue la conduite de l'élément matériel.

Le fait de dépourvoir une personne de sa propriété constitue le résultat de l'acte.

En tant qu'élément moral du crime, une intention particulière est requise : l'auteur du crime doit avoir l'intention de dépourvoir la victime de sa propriété.

Quand ce crime est réalisé sur Internet, ce dernier ne sert que d'intermédiaire pour faire tomber la victime dans l'erreur.[56]

L'auteur du crime propage ses triches et ses jeux par le moyen du réseau informatique. Le procédé le plus utilisé pour cela est la commercialisation de produits. L'intention de l'auteur de l'acte est de persuader les victimes d'envoyer de l'argent en contrepartie des produits, services et des bénéfices que la victime ne recevra jamais, ou au cas où il les recevra ces produits n'auront pas de valeur ou que très peu.

---

[55] ibid, p.5.
[56] ibid, p.13.

Les triches et les jeux "on-line" ne sont qu'une simple variation des jeux et triches traditionnels.

C'est la raison pour laquelle on peut imposer la responsabilité pénale à l'auteur de l'acte en se servant des éléments constituants du délit de fraude conventionnel.

L'utilisation du cyber espace en tant que moyen pour communiquer les triches et les jeux ou même en tant qu'instrument pour transmettre les fonds monétaires n'affectent en rien l'application de ces principes.

c) Le Vandalisme

Le vandalisme est le fait d'endommager ou de détruire la propriété d'autrui sans avoir le consentement selon le Droit américain.[57]

Les éléments constituants de ce délit sont les suivants :

Les faits d'endommager ou de détériorer, détruire le bien mobilier ou immobilier d'autrui sont les conduites.

Le résultat est que les biens d'autrui sont endommagés.

En tant qu'élément moral du crime une intention générale est suffisante.

L'élément d'illégalité de ce crime est l'absence du consentement du propriétaire.

Dans le cyber espace, l'acte de vandalisme est surnommé le "*cracking*"[58]. Cette expression dénote le processus selon lequel l'auteur gagne un accès illégal au système informatique d'autrui dans l'intention d'endommager ou détruire les logiciels qu'il contient.

Le type le plus commun du "cyber vandalisme" est la création et la propagation de virus.

Le "*cracker*" (celui qui fait du « *cracking* ») dans l'intention d'entraver le fonctionnement de l'ordinateur d'autrui, diffuse par l'intermédiaire des e-mails ou fichiers téléchargeables des virus ayant la capacité de détériorer le système informatique.

Là aussi, la seule différence entre les deux types de crimes est le moyen utilisé. Dans l'un, l'auteur utilise des outils informatiques pour endommager un bien dont il n'est pas le propriétaire, dans l'autre il se sert de sa force physique. Dés lors

---

[57] ibid,p.7.
[58] ibid, p.18.

que l'auteur agit dans l'intention de détériorer le matériel informatique d'autrui, les deux crimes présentent des caractères analogues.

En conclusion, les partisans de cette théorie disent que les comportements criminels dans le cyber espace, sont tous des actes préalablement définis par les lois pénales. Le cyberespace n'est qu'un nouveau support pour la réalisation des crimes conventionnels.

B. Existence des crimes spécifiques au cyberespace

Il convient de préciser tout d'abord que les partisans de cette théorie acceptent que pour la plupart des crimes, le cyberespace ne sert que d'intermédiaire. Cependant ils prétendent l'existence de certains cybercrimes ne présentant que très peu ou pas de points communs avec les crimes conventionnels et nécessitant la promulgation d'une loi spécifique. L'utilisation du cyberespace pour ces crimes, les affecte dans leurs éléments constituants, rendant ainsi impossible leur rapprochement aux crimes traditionnels. Ces crimes forment alors une catégorie distincte, indépendante pour laquelle un régime pénal particulier est nécessité.[59]

L'exemple qui est le plus familier aux partisans de cette théorie pour prouver l'existence de crimes spécifiques au cyber espace est celui de "*Mr Bungle et Lambda Moo.*"[60]

"Lambda Moo" est un canal de discussion situé dans le cyber espace et présentant des caractéristiques exceptionnels. Pour y participer, il faut d'abord devenir membre et s'approprier par la suite un pseudonyme et une carte d'identité virtuelle par lesquelles, les participants se feront connaître aux autres. La communication s'établit par l'intermédiaire des textes.

Dans cette affaire surnommé "*Lambda Moo & Mr.Bungle*", l'offenseur était un participant connu sous le nom de "*Mr. Bungle*" qui s'était muni d'une "poupée Voodoo", c'est à dire d'un programme qui lui permettait de "*spoofer*" les autres joueurs. "*Spoof*" est un terme qui dénote l'appropriation par un participant de l'identité d'un autre. Dans le contexte de « *Lambda Moo* » cela signifie qu'en

---

[59] ibid,p.25.
[60] Julian Dibbel, " A Rape in Cyberspace" (or Tiny Society And How to Make one) , www.levity.com/julian/bungle (06.12.2003).

donnant des commandes au "*voodoo doll*", son propriétaire peut s'approprier et agir sous l'identité d'un autre joueur.

« *Mr.Bungle* » se connecta un soir à « *Lambda Moo* » et utilisa ce logiciel pour s'approprier l'identité de plusieurs participantes, afin de les faire apparaître sur l'écran comme si elles étaient engagées dans des activités sexuelles humiliantes.

Les victimes de « *Mr.Bungle* » étaient choquées, traumatisées et n'arrivaient pas à comprendre comment il avait si parfaitement manipulé leur caractère. Elles avaient été mises dans une situation extrêmement humiliante et avaient été incapable de se défendre. Outragées par leurs souffrances, elles demandèrent que la peine capitale fût prononcée à l' encontre de « *Mr Bungle* » et son caractère fût ainsi annulé de « *Lambda Moo* ».

Mais les victimes ne se contentèrent de cette peine et prétendirent que le mal provoqué par « *Mr Bungle* » leur causa dépression et traumatisme semblables à celles des victimes de viol (sexuel) dans le monde réel.

Pour cela les défendeurs de l'existence de vrais cybercrimes qualifieront les actes de Bungle de "viol virtuel". Cependant, cet acte dite de "viol" ne présente rien de commun avec le viol du monde réel, car il n'y aucune attaque physique contre la victime. Il est impossible d'imposer une responsabilité pénale à "*Mr.Bungle*" même en modifiant la définition de "Viol" dans le code pénal. Dés lors nous sommes amenés à accepter l'existence de crimes spécifiques au cyber espace, formant une catégorie distincte et indépendante.

En conclusion des cyber crimes ne présentant aucun point commun avec les crimes conventionnels existent. Ces crimes ne se produisent que dans le cyber espace et nul part d'autre. Ainsi nous nous trouvons dans l'obligation d'élaborer des règles juridiques spécifiques pour les réprimer, les règles générales s'avérant insuffisantes pour assurer cette fonction. Nous sommes contraints de reconnaître l'existence de cyber crime "pures" et de créer un "droit des cybercrimes".

C. Notre Avis

1) Nous n'adhérons que partiellement aux deux théories. Il est vrai qu'une grande partie des crimes commis sur Internet, sont en effet des crimes conventionnels. Tel est le cas par exemple pour le délit de dol, fraude et dénonciation calomnieuse. Mais il existe une catégorie des crimes qui nécessite pour être

réprimée, la promulgation de nouvelles Lois. C'est ainsi que la Turquie a agi en 1991 pour punir les Hackers s'introduisant dans les systèmes informatiques pour accéder aux informations stockées à l'intérieur. Aujourd'hui on devrait agir de la même manière pour régler le problème de *Spam.*[61]

2) Cependant nous pensons que le cas de « *Lambda Moo* » et « *Mr Bungle* » ne fournit pas un bon exemple pour prouver l'existence de "cybercrimes purs."

Il serait aberrant de créer un crime de "viol virtuel" pour lutter contre ce type de comportements agaçants. De même cela irait à l' encontre de l'idéologie de l'Internet qui est de former une plateforme d'expression libre. La création d'un crime ne peut être envisagé que là ou existe un dommage suffisamment grave. Dans le cas de « *Lambda Moo* » et « *Mr.Bungle* », les victimes peuvent avoir subi un choc psychologique mais nous pensons que ce choc ne doit pas être trop grave étant donné que les événements prennent lieu dans un monde virtuel. Il faut préciser que ces femmes ont subi une agression indirecte : « *Mr.Bungle* » avait visé la personnalité qu'elles avaient créé dans le monde virtuel. Ces personnes se sont senties lésées car leur personnalité virtuelle ont été agressée et non pas elles !

Dans le cas « *Lambda Moo* » et « *Mr Bungle* », il sera plus juste et équitable de régler l'affaire dans le cadre de l'autorégulation, dans le cadre de la "Netiquette".[62]

3) Nous pensons qu'une classification dichotomique des cybercrimes résultant de la deuxième théorie et aussi proposé par David Lee Carter, professeur au département de Justice pénale à l'Université de l'Etat de Michigan, est adéquate aux caractéristiques de l'Internet.[63]

Celle ci tend à établir une distinction nette entre les cybercrimes en fonction de l'utilisation de la machine informatique, constituant « *sine qua non* »

---

[61] c'est l'action d'inonder de nombreux groupes de nouvelles Usenet ou groupes de discussions utilisant Interne, avec le même message inutile et souvent proocateur et sans rapport avec le sujet de discussion causant ainsi une véritable pollution des réseaux . Pansier – Jez,Op. Cit ,p.67.

[62] Il s'agit du code de bienséance de l'internet. Il a été mis au point par un groupe d'universitaires dans le temps ou l'Internet servait principalemet d'outil d'information.

[63] Pansier – Jez,Op. Cit ,p.12 .

cyber espace : soit l'instrument informatique est utilisé par le délinquant comme outil du crime conventionnel, soit il est la cible visée.[64]

Dans l'intelligence de cette conception nous pouvons opérer une distinction entre les principales infractions envers les biens et les personnes commises grâce à l'Internet et le domaine particulier de la cyber criminalité, phénomène radicalement nouveau dans lequel l'ordinateur apparaît comme la cible privilégiée du délinquant.[65]

Section II : Panorama des comportements criminels sur İnternet

Voici la liste des comportements criminels les plus fréquents sur İnternet. On peut les regrouper en trois groupes. Les crimes s'attaquant à la sécurité des systèmes d'information, les infractions allant à l'encontre des biens, et les infractions s'attaquant aux personnes.

Notons que la première catégorie est une liste exhaustive alors que la seconde et la troisième ne le sont pas. Cela est dû au fait que dans la deuxième et la troisième catégorie, l'İnternet soit le support des infractions énumérées.

Sous section I : Les crimes s'attaquant à la sécurité des systèmes d'informations

Ces crimes sont énumérés dans l'article 525 de l'ancien Code Pénal Turc et dans l'article 243 (et suivants.) du Nouveau Code pénal. İl faut noter que l'İnternet a considérablement favorisé leur prolifération.

---

[64] ibid.,p.12.
[65] ibid., p.12.

A) Structure

1) Généalogie

a) Apparition des hackers

Bien que ce soit le film de "*Wargames*" (1983)[66] qui révéla pour la première fois l'existence des hackers, une catégorie d'individus hautement qualifiés en technique informatique et fascinés par le cyber espace et son côte ludique, leur apparition date bien d'avant du 19ème siècle.

En effet, en 1878 aux Etats Unis à New Haven , dans l'immeuble de la Bell Telephone, une poignée d'employés adolescents commencèrent à écouter les conversations des abonnés et poussèrent la provocation jusqu'à y participer. Bell Telephone finit par congédier ces employés indélicats. Pour autant, les problèmes rencontrés par les abonnés ne cessèrent pas. Très vite les premiers «*pranksters* » (les farceurs) des nouvelles technologies utilisèrent les failles d'un système encore embryonnaire pour perpétrer leurs méfaits. Parmi ces failles nous pouvons citer, l'exploitation du partage des lignes pour s'immiscer dans les conversations d'autrui, l'impossibilité technique de retrouver l'émetteur d'un appel. Le téléphone n'a pas tardé à devenir le terrain d'exploitation des blagues de mauvais goût.

Un siècle plus tard, les «*pranksters* » cédèrent leurs places aux «*phreakers* » spécialisés dans la fraude à l'encontre opérateurs de télécommunication. Le «*phreaking* » – néologisme construit à partir des mots «*freak* » (mordu), «*fre e* » (gratuit) et «*phone* » (téléphone) consiste d'une part à ne pas payer les communications téléphoniques et d'autres part à pirater les lignes.[67] A l'origine du "*phreaking*", on trouve un vétéran de la guerre de Vietnam, John Draper. En 1965 Draper découvrit qu'un sifflet distribué en promotion dans le boites de céréales "*Cap'n Crunch*" émet une tonalité de 2600 mégahertz. Or cette fréquence audio était utilisée à l'époque par les réparateurs de téléphone pour accéder à une ligne depuis l'extérieur. Le sifflement déclenchait un signal qui commandait au

---

[66] Film portant a l'ecran un tres jeune pirate informatique à même de pénêtrer dans les systemes informatisés dela défense nationale américaine et de déclencher une guerre mondiale.
Ibid, p.99.

[67] "How crackers operate ?" http://home.actlab.utexas.edu/aviva/compsec/cracker/howcrack.html 23.12.2003.

central de ne pas facturer l'appel. Par la suite, John Draper, surnommé bien sûr "*Cap'n Crunch*" fût souvent arrêté pour piratage téléphonique.[68]

A la fin des années 70 avec la commercialisation des premiers micros ordinateurs, apparurent les premiers grands bidouilleurs informatiques. Leurs seules préoccupations étaient de pousser la machine dans ses derniers retranchements, optimiser le code source des logiciels et de créer de nouvelles applications. Soucieux de lever des défis techniques toujours plus difficiles, ils auraient pu en rester la, s'ils ne s'étaient pas associés aux phreakers avides de nouveaux terrains de jeux.[69]

La rencontre des pirates du téléphone et des pirates de l'informatique fût explosive.

Tous deux comprirent vite qu'en combinant leur connaissance ils allaient pouvoir se doter d'une compétence redoutable. C'est la complicité entre ces deux groupes qui fût à l'origine du « *Hacking* ».

b) Mise en place des réseaux organisés

L'apparition du « *hacking* » est donc antérieure à la généralisation de l'İnternet. En effet une des premières affaires de la cyber criminalité est révélée aux Etats Unis en 1981 lorsqu'İan Murphy, un étudiant de 24 ans et trois de ses amis utilisent une simple ligne téléphonique pour accéder à des fichiers stockées sur les ordinateurs du gouvernement fédéral américain et consulter des informations a caractère secret.[70]

Au milieu des années 1980, suivant le principe selon laquelle « L'Union fait la Force » les « *hackers* » s'organisèrent en groupes d'actions cohérents. İls fondèrent le groupe de *« Legions of Doom »* aux Etats Unis et le « *Chaos Computer Club* » en Allemagne.

L'apparition de la portion graphique de l'İnternet (le « *World Wide Web* ») marqua une évolution essentielle dans le développement du phénomène. Un moyen d'action privilégié pour pénétrer aux nouveaux systèmes fût alors offert aux

---

[68] Yannick Châtelain – Loick Roche , Hackers ! Cinquième Pouvoir , Paris, Maxima Laurent Du Mesnil-Editeur, 2002 ,p.14.

[69] İbid,p.15

[70] Pansier-Jez,Op.Cit, p.100

« *Hackers* » et ce fût également une opportunité pour multiplier leurs connexions criminelles en leur permettant d'échanger des mots de passe piratés, des astuces techniques ou des programmes d'intrusion.

L'Internet est devenu aujourd'hui un réseau de prédilection pour le « *Hacker* » et le principal support de la cybercriminalité.

2) Profil du « *Hacker* »

a) Définition

De l'anglais « *to hack* : hacher, tailler mettre en pièce », l'activité du « *hacking* » désigne à l'origine le passe temps commun des passionnés de l'informatique qui démontaient les logiciels afin de mieux en saisir le fonctionnement, d'en rechercher et d'en révéler les insuffisances tout en satisfaisant leur goût développé pour le défi intellectuel.[71]

Le phénomène « *Hacker* » a pris aujourd'hui une ampleur inédite. Depuis le bricoleur de génie bidouilleur impénitent à l'insatiable curiosité naturelle, au mercenaire se livrant à l'espionnage informatique, force est de constater que l'on se borne à désigner communément sans soucis de clarté, « *hackers* » l'ensemble des connaisseurs en informatique, suffisamment connaisseurs et habiles pour pénétrer là où on l'attendait pas.

Une classification[72] s'impose dés lors.

Il s'avère souhaitable de réserver l'appellation de « *Hacker* » à ceux dont l'unique motivation réside dans l'amélioration permanente des logiciels, agrémentés d'un aspect ludique.

A ce stade se profile déjà une première distinction entre le « *White hat Hackers* » et les « *Black Hat Hacker* ».[73] Le premier correspondant à la noble définition sus énoncée, ils sont des consultants en sécurité informatique, voire des cyber policiers. Ils ont un grand sens de la déontologie et de l'éthique. Ils se sont souvent donnés pour mission de défendre la liberté d'expression et le libre partage

---

[71] www.ifrance.com/chamandine/presentation1.html (17/12/2003).

[72] Châtelain – Roche , op.cit, p.68 .

[73] Les "*blackhat hackers*" sont aussi appelés "*cracker*"
ibid., p.67.

des connaissances. Pour cela, ils se battent sans répit contre les bureaucrates et les hommes d'affaires qui travaillent à s'emparer du Net.

Le second est le véritable pirate dénué de scrupules, qui se livrent à des activités franchement illégales. Ils n'hésitent pas à commettre des dégâts, à saccager lors de ses intrusions indélicates dans le réseau. Ils vivent dans la clandestinité[74] et sont largement rejeté par la communauté informatique. Les « *White Hat Hacker* » et les « *Black Hat Hacker* » forment ensemble la catégorie des élites.

Les « *Curious Joe* » sont une autre catégorie de « *hackers* ». Ce sont les passionnés de l'informatique, qui veulent tester leurs trouvailles et leurs outils sans intention foncièrement mauvaise. Mais souvent leur inexpérience les amène à causer de graves dégâts.[75]

Les « *Script Kiddies* » (un néologisme qui fait a la fois référence au script, c'est à dire écriture de programme, et au monde de l'enfance), néophyte en informatique ont pour seul objectif de nuire avec des programmes de « *hack* » « prêts à l'emploi » récupérés sur Internet. Ils sont méprisés par les véritables hackers car ils n'ont pas de réelles compétences informatiques.[76]

Les « *Wannabees* » constituent les nouvelles forces du hack. Ils ont une véritable ambition de recherche de la connaissance dans le milieu du hack et souhaitent passer dans les groupes des « Elites ». Pour ce faire ils commencent souvent par améliorer les scripts de « *hack* » existants. Lorsqu'ils développent leurs propres scripts originaux ils deviennent élites.[77]

D'autres termes font référence à des spécialisations plus ciblées encore.

Le « *Carder* » est celui qui démantèle le code d'accès du système central des cartes bancaires, tandis que le «*phreaker* » est passé maître dans l'art d'éluder le paiement de ses factures.[78]

---

[74]Les "*crackers*" ont tendance à se rassembler dans des communauté petites et tres secrètes. Ils aiment se considérer comme des hackers tandis que les vrais "*hackers*" les considere comme une forme de vie séparée et inférieure ! www.cybercrimes.net/property/cracking/cracking.html (06/12/2003).

[75] Châtelain – Roche , op.cit, p.68.
[76] ibid, p.68.
[77] ibid,p.69.
[78] ibid,p.70.

b) Les influences culturelles

Les influences culturelles du « *Hacking* » sont principalement dictées par la ligne idéologique propre au mouvement littéraire et philosophique du « *Cyber Punk* ». Le « *Cyber Punk* » naît de la peur du « *Big Brother* »[79] et se présente comme un contre culture. Il met en valeur un comportement subversif devant pousser à une prise de conscience de dangers inhérents à une gestion irréfléchie du cyber espace. Le postulat initial est le suivant : "Dans une société démocratique, il ne saurait y avoir de contrôle, ni de limite à la circulation de l'information numérique". L'idéologie « *Hacker* » repose donc sur le principe que toute information doit être libre et l'accès aux ordinateurs illimités et totales.[80] Suivant cette logique les gouvernements n'ont pas de vocations à restreindre la liberté d'expression sur les réseaux numériques. De nombreux « *Hackers* » ne se considèrent pas ainsi comme des criminels, mais comme de simples activités, suivant une règle éthique.[81]

c) L'âge

Les « *hackers* » sont en général des adolescents (lycéen ou étudiants) ou de jeunes personnes privées d'emploi.

Une étude mené par le « *Federal Bureau of İnvestigation* » (FBİ), il y a 10 ans en 1994, estime que la majorité des hackers les plus dangereux sont âgés de 18 a 35 ans, même s'il n'est pas exceptionnel qu'ils soient beaucoup plus jeunes.

---

[79] Big Brother est la personnalité créée par le romancier George Orwell dans son roman "1984". Celui ci symbolisait le dictateur dans le régime totalitaire, ayant confisqué a ses citoyrns toutes leurs libertés et les ayant ainsi réduits a des aliénés executant sans contester tous ses ordres.

[80] Le code des hackers : 1.La gratuité de l'information sur İnternet
2.La propriété intellectuelle doit appartenir a tous ceux qui ont la compréhension.
3.Les grandes entreprises ne sont pas dignes de confiance
4. Les grands gouvernements le sont encore moins
5. Toutes tentatives de légiferer pour rstreindre le cyberespace doit être combattue.
6. Le savoir faire technique est la vertu qui doit être la plus valorisée
Châtelain – Roche , Op.Cit , p.50 .

[81] Pekka Himanen , l'Ethique Hacker et l'Esprit de l'Ere de l'İnformation, Paris, Exils,Editeur, 2001 p.27.

d) Leurs motivations criminelles

Il est possible d'identifier cinq facteurs principaux déterminant des individus à entrer dans le monde de la criminalité informatique : des motivations sociales (besoin de reconnaissance), l'appât du gain, la vengeance, le besoin d'auto défense, et les motivations politiques.

aa) Les motivations sociales, techniques ou pédagogiques :

C'est le groupe le plus commun. Ces « *Hackers* » sont animés par le défi ou la volonté d'obtenir une certaine reconnaissance sociale permettant de s'insérer ou de reconnaître dans un groupe. Ils sont formés, en général, de « *Script Kiddies* » qui recherchent l'approbation de leur pair. Les nouvelles technologies leur donnent la possibilité d'accéder à un média de masse et ainsi de faire passer un message. Les sites Web hackés leurs servent de base promotionnelle et revendicative a leurs idées.

bb) L'appât du gain :

Ce groupe est composé d'individus sans grande moralité qui pénètrent les systèmes pour leur compte ou celui d'un tiers, dans le seul objectif de gagner de l'argent. En effet, la connaissance de réseaux informatiques offre des possibilités de détournement monétiques considérables.

Aussi le hacker Kevin Mitnick[82] avait détourné et utilisé prés de 20000 cartes de crédits avant son arrestation en 1995.

cc) La vengeance

Tel est le cas du responsable informatique qui suite à son licenciement en 1991, plaça une bombe logique[83] dans un programme installé sur les machines de l'employeur et causa la paralysie de l'entreprise pendant un mois.[84]

---

[82] Kevin Mitmick est le Hacker le plus connu et le plus respcté par ses pairs. Il est admiré par les hackers du monde entier : considéré comme un puriste, la communauté voit en lui un martyr quand d'autres voient un escroc. La justice américaine l'accuse d'avoir provoqué jusqu!a 80 millions de dollars de dégâts pour ses intrusions au sein de Motorola, Nokia et Sun Microsystems. Il est incarcéré à Los Angeles depuis fevrier 1995 www.ifrance.com/chamandine/media1.html (17/12/2003).

[83] programme de destruction à déclenchement différé.

[84] Pansier – Jez,op.cit , p.103.

dd) Le besoin d'autodéfense

Certains programmateurs utilisent des bombes logiques pour protéger leurs créations contre d'éventuelles contrefaçons.

ee) Les motivations politiques

Composé d'individus qui véhiculent des idéaux politiques forts, ce groupe prend pour cible les sites gouvernementaux et les sites des principales administrations d'un Etat pour faire passer ses messages et revendications.

Par exemple, en janvier 1999, le site du "Front National" français a été victime d'un piratage de sa page d'accueil par un certain "*raptor* 666". La nouvelle page d'accueil présentait une photo de Le Pen, barré de l'inscription "cette homme incarne une valeur... le racisme" ; le nouveau titre "Bienvenue au Front Facho" appelait à la dissolution du parti de sa milice.[85]

3) La typologie des agressions logiques

Les agressions logiques sont des attaques non physiques faites à l'encontre système informatique. Ces agressions regroupent des atteintes aussi variées que l'introduction de programmes virus, les intrusions, la paralysie ou le ralentissement des ressources de la machine.

a) Les agressions directes.

Ces agressions ont pour objectif de frapper un système d'information bien précis. On peut énumérer parmi les agressions directes les intrusions, le «*mailbombing* » et les bombes logiques.

aa) Le « *mailbombing* » ou délit d'entrave à un serveur.

Le « *mail bombing* » est l'une des méthodes les plus prisées. Ce méthode consiste à bloquer un serveur, un service ou la boite à lettre d'une personne en lui envoyant un nombre très élevé de messages électroniques. La victime reçoit un ou plusieurs messages volumineux qui auront pour conséquence de disjoncter la boite à message électronique.

---

[85] www.ifrance.com/chamandine/media2.html (17/12/2003).

On rencontre également ce type de nuisance dans les groupes de discussions. Le phénomène est communément appelé « *spamming* »[86] et se définit par l'action d'inonder de nombreux groupes de nouvelles Usenet ou groupes de discussion utilisant Internet, avec le même message, inutile souvent provocateur et sans rapport avec le sujet de discussion, causant ainsi une véritable pollution des réseaux.

bb) Les bombes logiques

Ce type de programme s'installe sur un ordinateur et attend un signal externe pour exploser et causer d'énormes dommages. Elles prennent souvent la forme d'un "cheval de Troie"[87]. Les dommages causés sont importants et entraînent une surcharge électrique causant la destruction matérielle de certains périphériques informatiques.

Parce qu'elles doivent être installées "physiquement" sur la machine, les bombes logiques sont des programmes de prédilection, par exemple des employés licenciés qui, ainsi se vengent de leur ancien employeur. Une fois installé sur l'ordinateur ciblé, la bombe logique attend un déclencheur, en quelque sorte "son heure" : elle peut être activée par le lancement d'une application, par l'identification de la machine quand elle se connecte a l'Internet ou au passage à une heure précise (01/01/2005 ou le jour de la Saint Valentin..)

---

[86] Le mot "*spam*" était utilisé par les Anglais pendant la seconde guerre mondiale pour décrire un "*corned beef*" au goût tres anglais fabriqué par la société "*Hornel Foods*" et que les americains parachutaient massivement sur la Grande Bretagne dans le cadre de l'une de leurs campagne "*humanitaire*". Le mot a été repris dans les années 80 par les Monty Pythons dans un de leur films. Dans l'une des scenes, on voit une serveuse de restaurant proposer systématiquement a ses clients : Nous avons ceci cela et du *spam,* cela,ceci et du *spam* (...)" et tous les clients reprendre en coeur "*spam, spam,spam, beautiful spam*". Aujord'hui la communauté internet s'est approprié le mot pour caracteriser tout ce qui est lourd et non digérable parce que non sollicité. Quand au terme "*spamming*" il correspond a l'acte lui même; celui qui l'accomplit étant appelé "spammeur".
Châtelain – Roche , op.cit, p 125-126 .

[87] La technique informatique du Cheval de Troie obéit strictement aux enseignements hélléniques.
"Brisés par la Guerre, repoussés par loes destins, les chefs des grecs, apres tant d'années ecoulées construisent, sous la divine inspiration de Pallas un cheval haut comme une montagne dont ils forment les côtes de Sapins entrelacés. C'est prétendent – ils une offrande a la déesse pour un retour heureux et le bruit s'en répand. Une élite de guerriers tirés au sort s'enferme furtivement dans ces flances ténébreux ; et le ventre du monstre jusqu'au fondde ses énormes cavernes se remolit de soldats armés. (Virgile, Enéide,II,v.13-20)
Il s'agit d'un programme qui se cache lui même dans un autre programme apparemment au dessus de tout soupçon. Quand l'utilisateur exécute ce programme, les instructions cachées s'exécutent parallelement. Le cheval de Troie tres difficile a localiser va se presenter sous des atours parfaitement innofensifs, voire même ludique. Néanmoins il peut causer des dommages irréparables. Une fois activé, le Cheval de Troie prévient son auteur (le pirate) et lui indique l'adresse IP de l'ordinateur. Ce dernier peut ensuite prendre le contrôle de la machine a distance et lire le courrier, voler des mots de passe ou détruire des fichiers. Pansier-Jez, Op.Cit, p.106 .

Parmi les plus connus on peut citer le « *Tchernobyl* », bombe logique activée le 26 avril 1999, jour du 18.ème anniversaire de la catastrophe nucléaire, avec des variantes se déclarant le 26 de chaque mois, « *Tchernobyl* » s'attaquait aux fichiers et aux disques durs des machines.

cc) Les intrusions

La commission d'un acte d'intrusion dans un système informatique est rarement une fin en soi et laisse présager une finalité criminelle différente : détournement, destruction, implantation de données.

b) Les agressions indirectes

Véhiculés de diverses manières, ces agressions ont pour objectif de frapper de manière aveugle.

aa) Le virus

Le virus est un petit programme ayant pour finalité d'altérer, d'endommager ou de détruire un système informatique.

Depuis l'invention de l'informatique le virus constitue le fantasme numéro un des utilisateurs.

Il y en aurait aujourd'hui plus de 60 000 et 2000 infections virales feront leurs apparitions chaque mois.

Trois ingrédients concourent au développement des virus : la multiplication des ordinateurs, leur connexion à Internet et le développement d'outils de création de logiciels (« *Java* », « *VBScript* ») à la portée des internautes avertis.

Remarquons néanmoins que tous les virus n'ont pas pour vocation de nuire pour le seul plaisir de nuire. Certains éditeurs de logiciel ont vu dans le virus une solution efficace contre la copie. Dés 1992 par exemple, la société « *Sega* » publiait « *Glock 360* », un jeu pour « *Amiga* »; qui s'il était piraté se bloquait et affichait un message sans ambiguïté :"Si je suis un « *hacker* », me voilà en difficulté. D'un autre côté si j'avais acheté ce jeu légalement, je n'aurai pas eu de problème. Si vous l'avez acheté et si cette erreur devait se produire, merci de nous faire un récapitulatif des détails de votre logiciel et de nous le retourner.[88]

[88] ibid, p.138.

Mais ces virus inoffensifs font exceptions et la justice poursuit les créateurs de virus.

bb) Le ver

Le ver est le virus des réseaux par excellence. C'est un programme qui s'auto reproduit à l'infini et se déplace au travers du réseau (Internet, intranet d'entreprise, réseau locale). Le ver n'a pas besoin de véritables "support physique" pour se déplacer. Il utilise par exemple, les adresses e-mail du carnet de la victime et se reproduit en se dupliquant pour chaque destinataire et ainsi de suite. Cependant si le récepteur e-mail n'ouvre pas la pièce jointe de son courrier, il ne risque rien. Au cas où il l'ouvre, le ver fouille de façon automatique dans les carnets d'adresses et il s'auto expédie via le réseau. Les vers se sont multipliés ces dernières années du fait du développement explosif des messageries électroniques. Parmi les vers les plus connus on peut citer "*I Love You*"[89]qui l'oeuvre de la démarche destructive d'une seule personne basées aux Philippines. Celui ci a affecté indifféremment des entreprises privées, des institutions publiques et aussi des simples particuliers. Il a infecté plusieurs millions d'ordinateurs en quelques jours et ses ravages sont estimés à 10 milliards de Dollars (!).

4) La Diversité des Menaces

a) Menace pour l'entreprise :

Les entreprises sont les premiers cibles des « *Hackers* » et risquent souvent très gros. Avec la nouvelle économie, la plupart d'entre elles sont présentes sur le Net et sont donc plus vulnérables. (C'est la bien un des paradoxes de la nouvelle technologie.)

L'entreprise en réseau augmente sa portance, sa visibilité et sa flexibilité mais parallèlement elle augmente les points d'entrée dans son réseau. Des informations confidentielles sur les clients mais aussi sur l'organisation interne de l'entreprise ou sur des nouvelles découvertes dans le domaine de la recherche et du développement sont alors disponibles sur le Net. Dés lors les attaques et les intrusions des réseaux ne sont pas que le fait des hackers mais elles proviennent aussi

[89] www.ifrance/chamandine/media.html (17/12/2003).

des firmes concurrentes…l'espionnage économique ainsi que le sabotage prennent avec l'Internet des proportions énormes. Dans des situations de guerre commerciales, les firmes embauchent des hackers et les utilisent pour désorganiser les firmes adverses. Elles peuvent par ce moyen, collecter des organisations techniques organisationnelles ou commerciales, substituer ces informations par des données inexactes ou simplement les détruire, elles peuvent également mettre hors service les serveurs et les autres moyens de communication avec la clientèle de l'autre firme.[90]

Les attaques de « *Hackers* » sont extrêmement nuisibles aux entreprises. Le manque à gagner ou la rupture du service peuvent peser très lourd pour l'établissement et ses clients usagers non seulement en raison des pertes financières considérables mais aussi parce qu'il risque de perdre sa crédibilité.

La soustraction frauduleuse des fichiers contenant des données confidentielles les inquiète particulièrement car elle menace les droits des particuliers.

Cette tendance du recours au cybercrime dans la guerre économique touche principalement le domaine des industries de pointe et des marchés émergeants.

b) La menace pour l'Etat

Des attaques logiques sont régulièrement menées à l'encontre des sites Web des organismes institutionnels dans un but de déstabilisation de l'action de l'Etat, en mettant une revendication à caractère politique.

La traque aux pirates trouve son point culminant aux Etats Unis. Depuis octobre 1999, plus de 150 systèmes informatiques fédéraux ont été visité illégalement et des informations classées "Top Secret" on été saisies.[91]

Récemment, des pirates informatiques ont réussi depuis Hong Kong à pénétrer le site Web de la Maison Blanche et à y laisser des messages revendicatifs dénonçant le bombardement par des forces de l'OTAN, de l'ambassade de Chine à Belgrade. En 1999, un rapport commandité par le Président Bill Clinton établissait qu'il était désormais possible de paralyser les infrastructures stratégiques du pays par des attaques directes ou indirectes grâce à l'effet domino. De telles attaques

[90] www.ifrance.com/chamandine/lutte2.html (17/12/2003).
[91] www.ifrance.com/chamandine/lutte1.html (17/12/2003).

pourraient être les symptômes d'actions hostiles de la part des puissances étrangères ou de groupes terroristes.[92]

Il existe au sein du FBI à Washington un centre de protection des Infrastructures Nationales chargé de coordonner la protection et la surveillance des réseaux informatiques.

Le président a demandé l'inscription de plus de 2 milliards dollars au budget de 2001 pour la protection des réseaux.[93]

Sur le plan militaire l'éventualité d'une guerre informatique n'est pas un postulat fantasque. Les postes informatiques militaires sont généralement liées aux réseaux et risquent de fournir aux pirates des opportunités importantes pour accéder à des informations militaires très confidentielles. Par exemple, durant la première Guerre du Golfe, l'armée américaine a révélé qu'un groupe de hackers hollandais s'était proposé de se mettre au service de l'action irakienne pour désorganiser le déploiement militaire américain moyennant la somme d'un million de Dollars. L'offre, qui fut repoussé présentait un degré de risque réellement élevé vu l'utilisation intensive qui était faite de l'Internet dans les transmissions militaires.[94]

En France le réseau informatique de l'enseignement et de la recherche, est protégé par le « *Computer Energy Response Team* », le CERT. Le CERT coordonne les efforts des spécialistes de la sécurité présents notamment au CEA (Commissariat de l'Energie Atomique). Il diffuse les alertes, avertit l'existence de nouveaux virus, fournit des documents sur les failles de sécurité des logiciels. Il existe également une équipe de "techno pompiers" destinés a recouvrir les administrations et les ministères : l'organisme est dirigé par le Service Central de la Sécurité des Systèmes d'Information (SCSSI), aux ordres de Matignon.

c) Le cyberterrorisme.

Imaginez ce scénario : en utilisant la technologie informatique, un terroriste interrompt les communications informatiques des plus grandes banques américaine, ainsi que celle des plus grandes institutions financières et du « *stock market* ». L'économie plongera dans une crise profonde. Par l'utilisation de la même technologie, les terroristes peuvent changer les formules des médicaments d'une

---

[92] Pansier – Jez, Op.Cit, p.111.
[93] www.ifrance.com.chamandine/lutte1.html.
[94] Ibid, p.112.

grande entreprise pharmaceutique, et y insérer des quantités dangereuses d'ingrédients chimiques. Des réactions allergiques et des "*over doses*" peuvent ainsi toucher et tuer des milliers. A peu près au même moment ces terroristes peuvent modifier la pression du gaz urbain et provoquer des explosions.[95]

Les experts de l'informatique sont d'accord sur le point que ces scénarios ne sont plus du phantasme hollywoodien. [96]

Le FBİ américain a défini le cyber terrorisme comme "l'utilisation illégale de la force et de la violence contre les personnes et la propriété dans l'intention d'intimider ou de forcer un gouvernement ou la population civile et de modifier les objectives sociales ou politiques"[97]

A ce stade il nous incombe d'effectuer une distinction entre les terroristes qui se servent de la technologie disponible et les "purs" cyber terroristes. Les premiers se contenteront d'agrandir leur arsenal de méthodes conventionnelles (prise d'otage, meurtre, explosions) avec de nouvelles méthodes comme le virus informatique. Les seconds parviendront aux mêmes résultats et éveilleront une peur au sein de la population, en utilisant la nouvelle technologie informatique. De plus les cyber terroristes atteindront leur but sans s'exposer à un danger quelconque : ils n'auront pas à franchir des frontières, à placer des bombes, à prendre des otages. Les terroristes du futur seront capables de provoquer plus de dommage avec un clavier et une souris qu'avec une bombe.

La leçon à tirer est que le cyber terrorisme est une menace imminente pour les pays technologiquement avancés.[98]

Afin de mieux saisir, l'étendue du cyber terrorisme, définissons le parallèlement au crime de terrorisme.

Le terrorisme est défini de la manière suivante dans l'article premier de la "Loi Turque de lutte contre le terrorisme" :

"La terreur est l'acte du membre d'une bande qui tente, de changer l'ordre politique, juridique, sociale, laïque, économique et les qualités de la

---

[95] Will Byar-Jimmy Sproles "examples of cyberterrorism" www.cs.etsu.edu./gotterbarn/stdntppr/cases/htm (22.12.2003).
[96] Tara Myrthri Raghavan "in fear of cyberterrorism : an analysis of the congressional response" http://www.jltp.uiuc.edu/recdev/articles/Raghavan/Raghavan.htm (21.05.2004).
[97] www.cybercrimes.net.terrorism/overview/page1.html (06/12/2003).
[98] Raghavan, Op.Cit.

République inscrits dans la constitution ; de détruire le pays, le peuple et l'indivisibilité de l'Etat; de mettre en danger l'existence de l'Etat et de la République Turcs; d'affaiblir, de détruire et de s'approprier l'autorité étatique; de soustraire les droits et les libertés fondamentaux; de menacer la sécurité interne et externe de l'Etat, ainsi que l'ordre public et la santé générale, en utilisant les moyens de pressions, de violence, d'intimidation, de découragement ou menace."

Les vols, les destructions, les extorsions, dégradations et détériorations, réalisé à l'aide de la technologie informatique peuvent être des actes de terrorismes lorsqu'elles obéissent à un mobile de terreur au sens de l'article 1er de la loi turque de la lutte contre le terrorisme !

Par exemple celui qui, membre d'un groupe de hacker, pénètrera le système informatique de la Grande Bourse d'İstanbul et déstabilisera, voire même détruira les ordinateurs par l'intermédiaire d'une bombe logique provoquant ainsi une crise économique très profonde en Turquie, ou celui qui s'introduira dans le réseau informatique interne d'İGDAS pour modifier la quantité ou la pression du gaz distribué à İstanbul mettant ainsi en péril la vie des milliers d'individus, sera poursuivi de crime de terreur au sens de l'article premier de la Loi concernée.

Le cyber terrorisme prend ainsi une existence légale à laquelle sont attachées des conséquences multiples. Citons la plus importante : les peines augmentent considérablement ! On peut rapprocher les comportements criminels terrorismes et cyber terrorismes sur bien des points et justifier ainsi l'utilisation du vocable "cyber terrorisme".

D'abord la spécificité du terrorisme aussi bien que le cyber terrorisme est de toucher un nombre indéterminé de victimes, suivant un processus plus ou moins aléatoires ce qui forme le caractère absurde et choquant de l'acte.

İl faut ensuite souligner l'importance de l'anonymat pour les victimes, et leur frilosité est un révélateur du terrorisme aussi bien que du cyber terrorisme. En effet les victimes sont marquées profondément par l'infraction. Par exemple, en France avant la loi no 86-1025 du 9 septembre 1986 concernant les actes de terrorisme et les attribuant un statut spécifique et plus répressif, on voulut constituer un jury pour juger les actes de terrorisme. Cela fut impossible tous ayant peur d'une éventuelle représaille. En cas de cyber terrorisme, le silence des victimes est la règle. İl s'agit surtout de ne pas se faire remarquer, de ne pas faire de la publicité et cacher

le fait que son système a subi une attaque. (Ce sera particulièrement désastreux pour une banque par exemple).

B) La criminalisation des infractions informatiques

Les atteintes aux biens informatiques ont longtemps été considérées comme une infraction particulière visant une catégorie particulière de biens.

Le développement de la criminalité informatique et en particulier du crime en réseau rendit nécessaire l'adoption de dispositions pénales particulières prenant en compte une certaine dimension technique.

Les enjeux de la sécurité informatique ont été prises en compte en 1991 en Turquie. L'insertion de l'article 525 dans le code pénal a permis de poursuivre les délits tels que l'accès frauduleux dans un système informatique, l'altération des données, la fraude informatique, le délit de faux commis avec un ordinateur et la contrefaçon informatique. L'arsenal juridique turc comprend donc cinq délits distincts visant les atteintes aux données informatiques. Nous n'en traiterons dans cette partie que deux : uniquement ceux qui visent l'atteinte aux systèmes informatiques.

1. L'İntrusion frauduleux dans un système de traitement automatisé des données (CPT art 525/a)

Cette nouvelle forme de criminalité consiste à pénétrer des systèmes à l'insu de leur administrateur.

L'incrimination est entièrement nouvelle dans le sens ou aucun texte n'appréhendait la situation auparavant.

Le texte de l'article concerné est comme le suivant :

« Celui qui saisit illégalement les programmes, les données ou un élément quelconque d'un système de traitement automatisé des données sera puni d'une peine d'emprisonnement d'une durée variable d'un à trois ans et d'une peine d'argent variable de 1 à 15 millions de Lires turques. »

La notion de "système de traitement automatisé des données" indique les systèmes informatiques, c'est à dire les ordinateurs.

L'Internet, étant un réseau composé d'ordinateurs inter reliés, correspond bien à cette notion.[99]

L'article 525 a/1 du code pénal turc est un exemple d'infraction commis à l'encontre du secret.

Le secret a une signification générale ici : c'est une information quelconque contenu dans le système informatique que l'on ne préfère pas exposer à autrui. La Loi ne requiert pas que l'information soit intime.

a) Les intérêts légitimes protégés :

Plusieurs intérêts légitimes sont protégés ici : premièrement ce sont les informations contenues dans le disque dur de l'ordinateur (ou les disquettes) qui bénéficient d'une protection contre les menaces et les attaques pouvant provenir de l'extérieur[100]. Deuxièmement le système lui même est prise sous protection puisque la saisie des informations ne peut s'effectuer qu'à l'occasion d'une ingérence au système. Troisièmement et en dernier lieu, la propriété est protégée[101]. Les droits matériels et intellectuels du propriétaire de l'ordinateur sur les informations que la machine contient, sont protégés ainsi que son droit de propriété sur la machine elle même.[102]

b) L'élément matériel de l'İnfraction :

Le sujet matériel de l'infraction est les programmes, les données ou autres éléments faisant partie du système de traitement automatisé des données.

La conduite se traduit par l'acte de saisir[103]. La saisie de l'information doit s'opérer illégalement.

La saisie ne signifie pas ici le fait de s'approprier, de copier ou d'utiliser les données. Ces actes sont le sujet d'une autre infraction. (CPT art 525/b). La saisie

---

99 Philippe Jougleux, La Criminalité dans le Cyberespace, Université de Droit d'Economie et des Sciences D'Aix Marseille, Faculté de Droit et de Science Politique d'Aix Marseille, Mémoire de D.E.A, Droit des Médias, Année de Soutenance 1999.

100 Caner Yenidünya- Olgun Değirmenci , Bilişim Suçları, İstanbul, Legal Yayıncılık San. Ve Tic.Ltd.Şti, 2003 ,p.53.

101 ibid, p.53.
102 ibid, p.53.
103 ibid, p.62.

est le fait d'apprendre, d'accéder à une information qui peut être sous la forme d'une donnée ou d'un programme.

La saisie exige que l'on pénètre directement ou indirectement le système. Le code pénal incrimine l'intrusion au système avec saisie illégale de données. La pénétration d'un système sans saisie d'information ne constitue pas un crime.[104]

Le résultat du crime est réalisé dés que l'acte est accompli. Il s'agit d'un crime dont l'acte et le résultat sont simultanés. Ainsi le crime est commis au moment même où l'information est saisie.

La tentation complète à ce crime est impossible.

La prescription commencera dés que la saisie sera faite.

c) L'élément moral de l'infraction

Certes, il s'agit ici d'une infraction intentionnelle. Pour que l'intrusion informatique soit répréhensible, il faut qu'elle soit délibérément voulue par un auteur ayant conscience de l'irrégularité de son acte au moment de sa commission. Cette intention doit prendre en compte la saisie d'une information précise. Mais une intention générale traduisant une curiosité pour prendre connaissance des données contenues dans un système, peut suffire à la réalisation de l'infraction.

L'infraction ne correspond pas à la réalité psychologique du « *Hacking* », le pirate cherchant souvent à entrer dans le système par jeu ou défi.

Les intrusions commises par imprudence ne seront donc pas poursuivis : par exemple, sur certains sites hackers peu fréquentable, existent de véritables portes ouvertes vers des sites payant ou à accès restreints. De simples liens hypertextes permettent ainsi d'accéder au coeur de ces sites par le biais d'une porte préalablement piratée (« *Backdoors* »)[105]. Tout internaute de peu d'expérience peut s'y glisser par une simple pression sur le bouton de sa souris et pénétrer le site par ce procédé illégal. En raison du manque d'une intention délibérée d'intrusion irrégulière, ces internautes ne seront pas considérés comme avoir commis le délit.

---

[104] Yılmaz Yazıcıoğlu, Kriminolojik Sosyolojik ve Hukuki boyutları ile Bilgisayar Suçları, İstanbul, Alfa Basım Yayım Dağıtım, 1997, p.236.

[105] Backdoor : "trou" de sécurité créé dans un ordinateur apres une premiere intrusion. S'attaquer aux backdoors d'un logiciel consiste a déceler les failles de sécurité inhrentes a tout programmes des lors que ceux ci sont constitués de milliers de lignes en code. Les pirates se servent donc de faiblesses structurelles des programmes pour les pénêtrer par effraction et effectuer les actes délictueux. Châtelain – Roche , Op.Cit, p.105&156.

d) L'illégalité :

L'illégalité fait partie des éléments de l'infraction. Si l'ordre juridique permet la conduite de l'auteur du crime alors l'acte ne sera pas poursuivi.

L'intention de l'auteur doit comprendre également cette illégalité.[106]

Le juge doit vérifier si l'auteur du crime était véritablement conscient de l'illégalité de son acte.

e) Applications:

Un procédé courant utilisé par les hackers consiste à "voler" l'adresse İP d'un utilisateur autorisé du système pour utiliser à son compte et pénétrer dans celui ci. Quelle que soit la perfection des manipulations déployées pour obtenir cet accès (en pratique souvent réalisé par l'intermédiaire d'une connection "*telnet*"). La validité apparente et technique de l'accès ne trompera pas le juge sur son caractère juridiquement frauduleux.

f) Les dispositions prévues dans le Nouveau Code Pénal Turc

L'intrusion frauduleuse dans un système informatique est régie à l'article 243 du nouveau Code Pénal Turc.

Le texte de la disposition est ainsi :[107]

« Celui qui s'introduit illégalement dans une partie du système informatique ou de sa totalité, ou y reste, sera puni jusqu'à deux ans de prison ou de peine pécuniaire judiciaire.

La peine de celui qui pénètre un système informatique dont l'utilisation est payante, pourra être diminué jusqu'à la moitié de la peine ci-dessus.

---

[106] Yenidünya- Değirmenci,Op.Cit,p.72.

[107] Le texte en turc de cette disposition est ainsi :

"Bilişim sistemine girme

MADDE 243- (1) Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam eden kimseye iki yıla kadar hapis veya adli para cezası verilir.

(2) Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi halinde, verilecek ceza yarı oranına kadar indirilir.

(3) Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, iki yıldan dört yıla kadar hapis cezasına hükmolunur." D'apres www.tcktasarisi.org (10.09.2004) .

Si les données contenues dans le système informatique s'effacent ou s'altèrent en raison de cette intrusion, la peine évaluera de deux ans jusqu'à quatre ans de prison. »

Les valeurs juridiques protégées ici, sont le droit au secret et le droit de propriété (sur le système informatique). La possibilité de porter atteinte au secret de la vie privée est incriminée ici. Il n'est pas obligatoire, que l'auteur du crime saisisse les données contenues dans le système informatique. Le seul risque de perception crée suffit pour le punir.

La conduite, constituant l'élément matériel de l'infraction est l'intrusion dans un système informatique et/ou l'acte d'y rester.

Le résultat est la prise de connaissance des données que le système informatique contient.

Nous avons affaire ici, à un crime dont la conduite et les résultats qui le composent (ses éléments composants) se reproduisent simultanément. C'est-à-dire, dés que l'acte d'intrusion dans le système informatique sera accompli, le résultat sera réalisé. Dans ce cas la tentative complète à ce crime n'est pas envisageable. Seul la tentative incomplète est possible.

En tant qu'élément moral du crime, une intention générale suffit : celui de vouloir pénétrer dans le système informatique et enfin d'y rester.

L'élément d'illégalité du crime, est l'intrusion illégale au système informatique. Cependant s'il y a un consentement du propriétaire du système, l'acte ne pourrait plus être incriminé.

La Loi sur le Nouveau Code Pénal Turc prévoit une situation dans laquelle la peine sera diminuée. C'est le cas où l'intrusion est réalisée envers le système informatique dont l'utilisation est payante, la peine peut diminuer de moitié.

D'autre part, si l'intrusion aboutit à la destruction ou l'altération des données, la peine devient plus grave. Elle augmente de deux à six ans de prison.

Les différences de cet article avec l'article 525a du présent Code pénal sont :

L'article 525a prévoit le saisissement des données contenues dans un système informatique. Seul l'intrusion sans saisissement de données n'est pas

incriminée. İci, même l'intrusion est prévue en tant que crime. Ainsi le champ d'application de ce présent article semble être plus large, agrandi.

2. L'altération des données (CPT art.525/b)

"Celui qui endommage ou altère ou efface complètement ou partiellement les informations contenues dans un système de traitement automatisé de données ou dans l'une de ses pièces, ou celui qui empêche ou fausse le fonctionnement du système dans le but de causer un dommage à autrui ou tirer du profit pour son propre compte ou celui d'un autre, sera puni de 2 à 5 ans de peines de prison et de 5 à 50 millions TL d'amende."

L'article 525/b du code pénal turc punit quiconque aura frauduleusement introduit, supprimé ou modifié les données contenues dans un système de traitement automatisé des données ou celui qui aura faussé ou entravé le fonctionnement de celui – ci.

Afin de mieux comprendre l'étendue du crime, il convient de définir la notion de données protégées. On entend par cela, une donnée informatique qui se résume à un ensemble d'instructions informatiques, codées en langage machine (suite de 0 et de 1). Tout programme en ce qu'il est un ensemble organisé de données en vue d'accomplir une tâche informatique précise est, en soi sujet de la protection pénale prévue, au même titre que tout fichier, seul ou organisé en base de données. Tout type de données résidant sur le système de traitement automatisé des données est protégé, quelque soit le support de stockage. Les bandes magnétiques, les disquettes et autres périphériques de stockage sont parties intégrantes du système de traitement automatisé des données. İl s'agit ici d'une forme spéciale du délit de destruction.

a) Les intérêts légitimes protégées

Le législateur a l'intention d'empêcher que le système informatique ainsi que ses programmes et les informations qu'il contient, soit agressé. Ainsi, les droits des personnes découlant de la propriété sont pris sous protection.

İl faut noter ici que la responsabilité pénale provenant du dommage causé n'exclut pas la responsabilité juridique décrite dans l'article 49 du Code Turc des Obligations.

b) L'élément matériel :

Le sujet du délit porte sur les éléments physiques et abstraits du système d'information. Les éléments abstraits sont des éléments comme les données et les programmes.

La conduite se manifeste par plusieurs actes. İl suffit de réaliser un afin que le crime soit réalisé.

- endommager : İl s'agit ici plutôt d'une agression physique. Elle peut se traduire par la destruction partielle ou totale du système de traitement automatisé des données ou par son endommagement au point de ne plus pouvoir s'en servir.

Notre sujet étant les crimes commis via İnternet, il n'est point envisageable que ce type d'agression puisse se reproduire.

-altérer : Ce sont les informations et les programmes du système de traitement automatisé des données qui y sont visés. Le législateur a l'intention d'incriminer les manipulations qui y sont faites sur.

- effacer : ce sont encore les informations et les programmes qui sont visés. On sous entend la destruction des données qui y sont enregistrées. Ce n'est cependant pas une destruction physique. C'est le fait de rendre le données méconnaissables ou d'enlever le lien virtuel nécessaire pour accéder a celles ci.

-entraver le fonctionnement : c'est empêcher le fonctionnement de l'ordinateur temporairement ou définitivement. Cela peut se traduire par les agressions physiques mais également par les agressions virtuelles. En matière d'attaque logique l'incrimination concerne principalement l'introduction volontaire dans un système de virus ou de bombes logiques.

-fausser le fonctionnement : İl s'agit de changer les fonctions que l'ordinateur devrait normalement accomplir. L'essentiel dans ce cas de figure, est que l'acte incriminé ait un effet sur la capacité de traitement de la machine. Le degré de la perturbation des opérations de traitement importe peu et l'entrave au fonctionnement ou le faussement d'un système concerne toutes les hypothèses de ralentissement ou de paralysie du système informatique.

Le résultat du crime est réalisé dés que l'un des actes sus cité est accompli. " La conduite et le résultat sont simultanés".

La tentation complète est impossible.

La tentation incomplète peut être envisagé si l'acte est divisible.

c) L'élément moral

Une intention particulière est requise. L'acte doit être accompli dans l'intention de causer du dommage à autrui ou de tirer du profit pour son propre compte ou celui d'autrui.[108]

Sont ainsi exclues les transmissions automatiques de fichiers virus par courriers électroniques. De même, le caractère intentionnel du délit s'oppose à ce que soient réprimées les communications de fichiers corrompus par des virus à l'insu de l'auteur.

d) Applications :

Le législateur permet d'envisager de manière autonome, le cas de figure le plus fréquent en matière d'atteinte à la sécurité d'une entreprise. Un individu travaillant pour l'entreprise a forcément accès au réseau de celle ci. Si les notions d'accès et de maintien ne permettant pas d'organiser une répression efficace, les notions d'entrave ou d'altérations envisagée par l'article 525/b autorisent à poursuivre l'employé peu scrupuleux. L'hypothèse la plus courante est celle de l'insertion d'une bombe logique par le salarié qui pourra ainsi se venger rétroactivement en cas de licenciement.

Cet article permet la poursuite des manipulations des pages Web.

Par exemple si le serveur Web d'une entreprise assez connue est manipulé, on appliquera l'art 525/b du code pénal à l'encontre de l'auteur de l'acte.

e) Les dispositions prévues dans le Nouveau Code Pénal Turc

La disposition prévue dans le Nouveau Code Pénal est comme le suivant ;

« Celui qui empêche le fonctionnement d'un système informatique, le détériore, ou d'une manière illégale y installe de nouvelles données, envoie les

---

[108] Un virus informatique au nom de "happy 99" prend ainsi furtivement le conrôle de la messagerie de sa victime et se propage en envoyant automatiquement des courriers électroniques à toute les personnes referencees sur le carnet d'adresses. Pansier – Jez, Op.Cit, p.97.

données existantes vers un autre système, les rend inaccessible, les altère, les détruit sera punis d'un à deux ans de prisons.

La peine augmentera de moitié si ces actes sont réalisés envers un système informatique appartenant à une banque, une institution de crédit ou une institution ou organisation publique.

(...) »

La valeur juridique protégée ici est le droit à la propriété.

L'élément matériel de l'Infraction est une conduite à choix multiples. Ces choix sont : empêcher le fonctionnement d'un système informatique, le détériorer, y installer des nouvelles données, envoyer les données existantes vers d'autres systèmes informatiques, rendre les données inaccessibles, les altérer, les détruire.

Il suffit de commettre un de ces actes afin que le crime soit réalisé.

Les actes et leurs résultats se reproduisent simultanément.

Seule la tentative incomplète à ce crime est possible.

L'intention générale de porter atteinte au fonctionnement du système suffit.

Sous Section II : Les Principales infractions commises envers les Biens et les Personnes par l'intermédiaire de l'Internet.

Les crimes que nous allons aborder maintenant sont ceux qui sont les plus fréquemment commis sur Internet. Dans ce cas, l'Internet sert de support aux crimes conventionnels, du coup, cette liste n'est pas exhaustive.

L'intérêt de cette partie est de voir les moyens de violation et de contrôler si les textes législatifs prévoient leur violation par le moyen de l'Internet.

A. les crimes informatiques s'attaquant aux Biens.

Ces crimes se subdivisent en deux : ceux qui s'attaquent aux biens immatériels et ceux qui vont à l'encontre des biens matériels.

1. Les crimes s'attaquant aux Biens immatériels

Les crimes s'attaquant aux biens immatériels sont deux types : ceux qui vont à l'encontre des droits d'auteur et ceux s'attaquant aux droits découlant de la marque.

a. Les droits d'auteur

Le droit de la propriété intellectuelle et artistique a été le premier domaine dans lequel l'Internet a posé de problèmes juridiques sérieux.

Le droit pénal doit se servir ici de cette branche du Droit, car la répression ne pourra s'effectuer que si les données modifiées, copiées ou autre constituent des œuvres au sens de la Loi portant sur la Protection de la Propriété İntellectuelle et Artistique (LPPİA).

aa. Les Notions Principales

Une simple information ne bénéficie pas de la protection du code de la propriété littéraire et artistique. Le terme piratage n'a de sens que si la cible est une œuvre.[109]

La Convention de Bern, qui est une des sources internationales principales du droit de la propriété littéraire et artistique[110] ne donne aucune définition de l' « œuvre ». Elle se contente d'énumérer dans son deuxième article les différents types d'œuvre et de préciser les deux critères qu'elles devront tous porter :

- l'originalité
- elles doivent être les fruits d'une réflexion intellectuelle reproductive.

La Loi turque no : 5846 portant sur la protection de la propriété littéraire et artistique[111] définit la notion d'œuvre dans son premier article :

L'œuvre d'art est selon cet article, le produit d'une réflexion et de l'art, appartenant au domaine de la Littérature, de la Science, de la Musique, des Beaux Arts ou du Cinéma et portant les caractéristiques de son auteur.[112]

---

[109] Ünal Tekinalp , Fikri Mülkiyet Hukuku, 2.Bası, İstanbul, Beta Yayınevi, 2002, p.91.
[110] ibid, p.63.
[111] Cette Loi a été promulguée en 1951 suite à l'adhésion de la Turquie a la Convention de Bern en 1948. Elle a été amendée quatre fois jusqu'a aujourd'hui. Ces amendements ont été réalisées en 1983, en 1995, en 2001 et dernièrement en 2004.

Le propriétaire de l'œuvre ou son auteur, est selon l'article 1/B de la LPPİA, la personne physique ayant créé l'œuvre. İl est celui qui va pouvoir bénéficier de la protection procurée par cette Loi.

L'auteur de l'œuvre d'art dispose des droits moraux et patrimoniaux sur son œuvre.

Les droits moraux reconnaissent à l'auteur des droits perpétuels inaliénables et imprescriptibles au respect de son nom, de sa qualité d'auteur et de son œuvre. [113]

Les principales attributions de ces droits sont :

- le droit de divulgation c'est à dire la faculté de rendre ou non l'œuvre publique, aux conditions et suivant les procédés que l'auteur souhaite.[114]

- le droit de paternité reconnaissant à tout auteur d'œuvre originale le droit de se faire connaître publiquement en sa qualité d'auteur de l'œuvre divulguée et l'obligation pour tout utilisateur de l'œuvre d'en citer l'auteur.[115]

- le droit au respect de l'œuvre permettant à l'auteur de s'opposer à toute modification, suppression ou adjonction susceptible de dénaturer son œuvre.[116]

Les Droits patrimoniaux sont caractérisés par la propriété de l'auteur sur son œuvre : ce sont les droits exclusifs et opposables à tous et conférant à son titulaire la faculté de l'exploiter par représentation ou reproduction sous quelles formes que ça soit et d'en tirer un profit pécuniaire.[117]

Les principales prérogatives de ce droit sont :

- le droit de représentation, c'est-à-dire la communication de l'œuvre par un quelconque procédé. Il s'agit d'une très large acceptation qui comprend aussi bien l'exécution directe de l'œuvre par des interprètes que la communication a l'aide de tous supports matériels.[118]

---

[112] Tekinalp, op.cit,p.100.
[113] « Droits d'auteur » www3.teaser.fr/~jjrey/udp/97-98/Droits_d_auteur.html. (14.07.2004).
[114] LPPİA art.14.

[115] LPPİA art.15.

[116] LPPİA art.16.
[117] "Droits d'auteur", op.cit.
[118] LPPİA art.24.

- le droit d'enregistrement à savoir la faculté reconnue au créateur d'autoriser la fixation matérielle de son œuvre sur les supports et par les procédés de son choix en vue d'une communication indirecte au public.

- le droit d'émission conférant à l'auteur la faculté de vendre, de louer, de prêter ou de distribuer les copies de son œuvre par des voies semblables.[119]

- le droit d'adaptation, d'arrangement et d'autres transformations.

Seuls les auteurs peuvent jouir du droit exclusif d'autoriser les adaptations, arrangements et d'autres transformations de l'œuvre.[120]

- le droit à la radiodiffusion par radio, par câble ou par satellite.[121]

- le droit de reproduction sous diverses formes : la faculté de reproduire son œuvre, d'autoriser sa fixation matérielle sur les supports et les procédés de son choix en vue d'une communication indirecte au public est reconnue au créateur de l'œuvre.

Les prérogatives patrimoniales sont reconnues a l'auteur durant toute sa vie et a ses ayant droits 70 ans après son décès.[122]

bb. Les atteintes aux droits d'auteur sur İnternet

Les atteintes aux droits d'auteur sur İnternet vont être examinées de deux différentes points de vue : les violations aux droits d'auteur sur le site Web lui-même et sur le contenu du site web.[123]

aaa. Les atteintes aux droits d'auteurs sur le site Web lui même.

En premier lieu, il convient de se demander d'abord si les pages Web sont des œuvres.

En France, également adhérente à la Convention de Bern, les juges se sont prononcés à l'occasion de l'affaire dénommée Cybion.[124]

---

[119] LPPİA art.23 .

[120] LPPİA art.21.

[121] LPPİA art.25.

[122] LPPİA art.27.

[123] Özdilek Osman, İnternet ve Hukuk, İstanbul, Papatya Yayıncılık, 2002, p.72.

[124] T.C de Paris, 9 février 1998, affaire Cybion contre Qualistream.
D'apres Jougleux, op.cit, p.43.

En l'espèce, une entreprise avait repris certaines pages d'un site appartenant à une entreprise concurrente.

Selon cet arrêt, la plupart des pages Web doivent être considérées comme des œuvres, sauf dans certains cas, cette qualification peut lui être entièrement refusée. C'est le cas des pages essentiellement techniques, notamment de la page insérée par l'administrateur du site pour prévenir que l'internaute s'est heurté l'erreur 404 : disparition du site recherché.[125]

Une page Web est composée d'une série de code « Html ». A l'origine ce langage est conçu pour diffuser des textes. A un niveau d'utilisation supérieure, s'ajoute au langage « html » des langages plus sophistiqués tels que les « *Applets* » (langage « *Java* ») et les Scripts (langage « *Vbscript* »).

Appréhendée sous cette angle, la page Web pourra constituer une sorte de logiciel, s'appliqueraient alors les règles spécifiques régissant ce type d'œuvre. Les logiciels informatiques sont énumérées à l'article 2/a-1 de la Loi no 5846 parmi les œuvres scientifiques et littéraires. En effet, tous les éléments constituant le site Web, c'est-à-dire, les images, les graphiques, les sons et la musique ont la qualité d'œuvre au sens de la Loi no : 5846. Le site Web peut ainsi être considéré aussi comme une compilation d'œuvre d'art[126] ou comme une base de données au sens de l'article 6 alinéa 11.[127]

Parmi les menaces récentes sur le site Web, la plus importante est le lien hypertexte.[128] Le lien hypertexte est l'instrument qui permet à l'utilisateur de naviguer entre les sites en empruntant des ponts entre les pages Web. İl représente l'ossature de l'İnternet.

La pratique s'est instaurée très vite d'instaurer des liens hypertexte vers d'autres sites, que ça soit ses sites préférés ou des sites abordant des sujets analogues.

Ces liens hypertextes doivent être créés avec l'autorisation du créateur du site destiné, un transfert des droits patrimoniaux doit être opéré.

Il existe plusieurs catégories de liens hypertextes.

Tout d'abord il faut opposer le lien dirigé vers une page Web à l'intérieur du même site, sans conséquence juridique, et le lien extérieur.

---

[125] İbid.,p.43.
[126] Tekinalp,op.cit,p.116.
[127] Özdilek, op.cit,p.74.
[128] Aussi appelée "*linking*" en anglais.

Le lien extérieur se décompose en plusieurs formes. Le simple « *linking* » ou le référencement à une page secondaire, c'est-à-dire le référencement à une page d'accueil ; le « *deep linking* » ou référencement secondaire qui signifie le renvoi à une autre page du site ciblé et le « *inline linking* » qui est l'utilisation plus raffinée du lien hypertexte consistant à pointer non pas à des pages Web, mais aussi bien à du son, à une image, une vidéo pour l'intégrer artificiellement à sa page : l'image et le son apparaîtront comme faisant partie intégrante du site.

Enfin le « *Framing* » ou le cadrage qui est une technique indépendante de référencement permettant d'afficher simultanément plusieurs pages Web, chacune occupant une partie de l'écran donnant par conséquent l'impression d'un tableau.

Il faut noter une certaine gradation, alors que le simple « *linking* » laisse intact la philosophie de l'İnternet puisqu'il renvoie à la page de garde censée de comporter toutes les informations de l'auteur, le « *deep linking* » est un peu plus agressif mais peut être toléré.

Le « *inline linking* » infuse un doute quand à la propriété de la page Web et donne l'impression d'une récupération illégitime du travail d'autrui.

Le «*framing* », incorporant complètement la page, à moins qu'il ne soit assorti d'une mention portant le nom du propriétaire, semble totalement frauduleux.

Les juges américains se sont prononcés au sujet du «*framing* », à l'occasion de l'affaire « *Total News* » en 1997[129]. En l'espèce, « *Total News* » contenait une compilation de liens renvoyant à des sites de journaux tels que le « *Washington Post* » et six autres sociétés éditrices de journaux en ligne. Ces sociétés l'ont assigné. Les juges ont effectivement constaté une violation des droits patrimoniaux. Une transaction est alors intervenue entre les parties au termes de laquelle « *Total News* » a renoncé à encadrer les sites des journaux en ligne, tout en conservant le droit d'établir des liens hypertextes simples vers ces sites à condition d'utiliser les noms, en toute lettre, des sites liés et sans utilisations de leur logo.

De même, en février 1999, une affaire a opposé la société « *Ticketmaster* » à la société « *Microsoft* »[130]. En l'espèce, « *Microsoft* » avait placé un lien profond sur son site « *sidewalk* ». « *Ticketmaster* » a allégué un acte de

---

[129] www.adbs.fr/site/publications/droit-info/mai.2000.pdf "La Jurisprudence : Quelques affaires marquantes" (05.05.2004).

[130] Erol Karaoğlu, « Bir web sitesine diğer bir web sitesinden bağlanma (=linking) ve doğurduğu hukuksal sorunlar » www.hukukcu.com/bilimsel/kitaplar/linking.htm (06.10.2003).

parasitisme commercial ainsi que la violation de ses droits patrimoniaux. Un accord a été conclu et « *Microsoft* » a été obligé de réorienter son trafic vers la page d'accueil de Ticket master.

Donc le « *deep linking* » et le « *inline linking* » contreviennent au droit de représentation (droit patrimonial) et au droit de paternité (droit moral) de l'auteur du site lié puisque la page et le fichier paraissent incorporés au site.

Pour éviter ce genre de violation, il semble nécessaire de conclure un contrat de cession des droits patrimoniaux ainsi que de mentionner l'auteur de l'œuvre divulguée. Sinon il semble inévitable, du moins en Turquie, de s'exposer aux sanctions prévues dans le cadre des articles 71 et 72 de la Loi no 5846.

bbb. Les atteintes aux droits d'auteur sur le contenu du site Web

Les codes html, les textes, les images et les graphiques ainsi que les musiques et les poèmes que les sites Web contiennent sont considérés comme des œuvres d'art (compilation d'œuvre) et sont protégés par la Loi no 5846 en Turquie.

Le cheval de bataille au sujet des droits sur le contenu des sites Web fut incontestablement le « *MP3* ».

Le « *MP3* » signifie « *Motion Picture Experts Group Audio Layer 3* ».

Au départ, le « *MP3* » était un format de fichier électronique utilisé pour compresser les documents visuels sur ordinateur. Il fut ensuite développé de façon à compresser les enregistrements sonores en conservant une qualité d'écoute équivalente à celle de l'enregistrement numérique.

La transformation d'une œuvre musicale au format « *MP3* » sans la présence d'un contrat de cession des droits patrimoniaux ou en l'absence d'une licence d'utilisation, constitue violation des droits patrimoniaux, en particulier des droits d'émission et publication.

L'affaire le plus connu en matière de « *MP3* » est celui opposant « *A&M Record Inc.* » à « *Napster* »[131]. En l'espèce « *Napster* » était un catalogue central permettant aux internautes d'échanger des fichiers « *MP3* ». Par ce moyen le site recevaient plus de 100.000 (!) visites par jour d'internautes qui pouvaient gratuitement écouter et télécharger le « *CD* » format de la chanson, voire graver le « *CD* » audio de leurs rêves. L'industrie Américaine du disque et ses représentants de

[131] Nicolas Vermeys, "L'union fait la force pour Napster" www.juriscom.net.actu.achv./200011.htm (05.05.2004).

la « *RİAA*[132] » ont violemment réagi : « *Napster* » fût l'objet de plaintes pour violation des droits d'auteur. Le 26 juillet 2000 « *Napster* » est condamné par la « *United States District Court of San Francisco* » à suspendre ses activités en attendant qu'un tribunal se prononce sur le fond. C'est en plein milieu de cette bataille judiciaire dans l'angoisse d'un procès risquant de mettre fin à ses activités que « *Naspter* » conclua un accord, le 31 octobre 2000, avec la société allemande « *Bertelsmann* » pour créer un service d'échange de fichiers musicaux par abonnement.

De violations semblables sont aussi réalisées par l'intermédiaire des technologies « *DİVX* »[133]. Ce dernier est un système de compression de fichiers numérique semblable au « *MP3* » qui permet d'enregistrer sur un CD plus deux films cinématographiques. Le partage des fichiers sous format « *DİVX* » est réalisé par l'utilisation des logiciels tel que le « *Gnutella* » ou le « *Scour Exchange* » ou par l'intermédiaire des groupes de nouvelles et des canaux de discussions tels que l' « *IRC* ». Ainsi beaucoup d'œuvres cinématographiques dont le coût pouvait être évalué à des millions de dollars, ont été distribuées gratuitement sous formes de fichiers visuels compressés par l'intermédiaire de l'İnternet.

Enfin un dernier type de violation sont les sites « *Warez* ». Les sites « *Warez* » sont des réseaux organisés, munis de leur propre règle de fonctionnement offrant aux utilisateurs la possibilité de télécharger des logiciels piratés c'est à dire contrefaisants. Le terme « *Warez* » est lui-même une sorte de code pour marquer tout ce qui est illégal (ex : « *downloadz* »-« *gamez* »-« *mp3z* »). Ces codes servent à apporter la connotation souhaitée à la requête des moteurs de recherche. İl faut noter cependant que les sites Warez n'ont pas une fin bénévole : en général, le créateur du site « *Warez* » insère des bandeaux de publicité de bas de gammes (pornographique). Il est payé au nombre de personne visitant le site au meilleur des cas pour lui ; ou le plus souvent au nombre de personnes ayant cliqué sur le bandeau qu'il héberge sur sa page ayant par conséquent actionné le link portant vers le site Web publicitaire.

Le créateur du site « *Warez* » prend le risque d'être poursuivi pour délit d'exportation d'ouvrages (logiciels informatique) contrefaits ce qui va l'emmener à chercher toutes sortes de moyens techniques et juridiques pour se protéger. Dans cet

---

[132] "Recording İndustry Association of America".

[133] Özdilek, Ali Osman « Film Korsanlığı ve İnternet » www.hukukcu.com/bilimsel/kitaplar (06.10.2003).

objectif la meilleure solution pour le titulaire du site « *Warez* » est de créer des sites miroirs. Il s'agit de démultiplier les adresses İP où on peut accéder à un même page de référence en la confiant à plusieurs entreprises d'hébergement de nationalité différentes si possible. Ainsi le contenu démultiplié et litigieux des sites Warez sera intouchables judiciairement et l'auteur restera en sécurité.

cc. La répression des atteintes aux droits d'auteur.

Bien que n'étant pas prévue et promulguée dans un contexte dans lequel l'İnternet existait, nous avons déjà évoqué qu'il est possible de protéger les droits d'auteur des agressions, à l'aide des dispositions de la Loi Turque no 5846 sur la Propriété İntellectuelle et Artistique. Celle-ci ne contient en effet aucune disposition restrictive quand aux supports utilisés par l'agresseur, et elle n'a qu'une exigence : la cible du crime doit être une œuvre.

Nous avons vu aussi que la plupart des agressions à ce sujet (le « *linking* », le «*framing* », le « *MP3* », le « *DİVX* », et le « *Warez* ») posaient une problème de violation des droits patrimoniaux, sauf le « *deep linking* » et le «*framing* » entraînaient aussi la violation des droits moraux.

Abordons maintenant les sanctions prévues en Turquie par la loi en question, en cas d'atteinte à ces droits.

aaa. Atteintes aux droits patrimoniaux.

La violation des droits patrimoniaux est régie par l'article 72[134] de la présente Loi.

---

[134]Le texte en turc de l'article concerné de la Loi est ainsi :

"Madde 72. *– (Değişik: 3.3.2004-5101/18) Bu Kanuna aykırı olarak kasten; 1. Aralarında mevcut bir sözleşme olmasına rağmen bu sözleşme hükümlerine aykırı olarak bir eser veya işlenmelerinin kendi tarafından çoğaltılmış nüshalarını satan veya dağıtan kişiler hakkında, üç aydan iki yıla kadar hapis veya onmilyar liradan ellimilyar liraya kadar ağır para cezasına veya zararın ağırlığı dikkate alınarak her ikisine birden, 2. Hak sahibinin izni olmaksızın bir eseri ve çoğaltılmış nüshalarını, bu Kanunun 81 inci maddesinin yedinci fıkrasında sayılan yerlerde satan kişiler hakkında üç aydan iki yıla kadar hapis veya beşmilyar liradan ellimilyar liraya kadar ağır para cezasına veya zararın ağırlığı dikkate alınarak her ikisine birden, 3. Hak sahibinin izni olmaksızın; a) Bir eseri herhangi bir şekilde işleyen, b) Bir eseri herhangi bir şekilde çoğaltan, c) Bir eseri herhangi bir şekilde yayan, d) Bir eserin nüshalarını yasal veya yasal olmayan yollardan ülkeye sokan ve her ne şekilde olursa olsun ticaret konusu yapan, e) Bir eseri topluma açık yerlerde gösteren veya temsil eden, bu gösterimi düzenleyen veya dijital iletim de dahil olmak üzere her nevi işaret, ses ve/veya görüntü iletimine yarayan araçlarla yayan veya yayımına aracılık eden, Kişiler hakkında iki yıldan dört yıla kadar hapis veya ellimilyar liradan yüzellimilyar liraya kadar ağır para cezasına veya zararın ağırlığı dikkate alınarak her ikisine birden hükmolunur."* D'après www.ilesam.org.tr/telif html (15.08.2004).

« Celui qui contrevenant intentionnellement à cette Loi ;

1. Agit à l'encontre des dispositions du contrat qu'il a conclu avec l'auteur de l'oeuvre, et vend ou distribue les copies, qu'il a lui-même reproduit, d'une œuvre originale ou d'une œuvre adaptée, sera puni de 3 mois à deux ans de prisons ou de 10 milliards à 50 milliards de Lires Turques d'amende ou si le préjudice est trop grand des deux à la fois

2. Vend, sans l'autorisation de l'auteur, une œuvre ainsi que ses copies dans les lieux énumérés par l'article 81 alinéa 7 de la présente Loi, sera puni de 3 mois à deux ans de prisons ou de 5 milliards a 50 milliards de Lire Turque ou si le préjudice est trop grand des deux à la fois,

3. Celui qui sans l'autorisation de son auteur,

a. Adapte une œuvre,

b. Reproduit une œuvre,

c. Divulgue une œuvre,

d. Exporte par des voies légales ou illégales les copies d'une œuvre et les commercialise,

e. Représente ou montre une œuvre dans un lieu public, organise cette représentation ou divulgue ou sert d'intermédiaire à la divulgation par l'intermédiaire des outils servant à la conduction des voix, des images et des signes de toutes sortes, y compris par les voies digitaux,

Sera puni de 2 à 4 ans de prisons ou de 50 à 150 milliards d'amende ou si le préjudice est trop grand des deux à la fois. »

Cet article de la Loi a été amendé en 2004. Le premier et le deuxième paragraphe ont été rajoutés, cet article régit désormais trois types de crimes différents ayant tout de même un point commun : la violation des droits patrimoniaux de l'auteur. D'autre part il faut ajouter que les peines ont été alourdies.

L'élément matériel de la première infraction est constitué par des actes est à choix multiple : vendre ou distribuer les copies d'une œuvre originale ou d'une œuvre adaptée. Il faut noter aussi que l'acte et son résultat sont simultanés.

Une tentative incomplète à ce crime est envisageable .L'auteur du crime peut avoir terminé les actes de préparations (la reproduction de l'œuvre) et avoir fait les démarches nécessaires pour vendre ou distribuer les copies sans pour autant y réussir.

En ce qui concerne l'élément moral de cette infraction, celle-ci est intentionnelle. La loi requiert une intention générale

L'élément d'illégalité du crime est la violation des dispositions du contrat et le manque de consentement de l'auteur de l'œuvre.

Les peines prévues sont soit alternatives soit cumulatives en fonction de l'importance du préjudice.

En ce qui concerne la deuxième infraction prévue dans le texte du même article, son élément matériel est la vente des copies d'une œuvre. L'acte et son résultat sont simultanés.

Une tentative incomplète à ce crime est possible.

En ce qui concerne l'élément moral de cette infraction, celle-ci est intentionnelle aussi.

L'élément d'illégalité est le manque de consentement de l'auteur de l'œuvre.

Les peines prévues sont soit alternatives soit cumulatives en fonction de l'importance du préjudice

La loi prévoit une condition de la réalisation à ce crime : la vente doit être réalisé dans les lieux prévus par l'art 81 al 7. Ces lieux sont les places publiques, les marchés, les trottoirs, les ponts et dans les lieux semblables.

Donc ce crime ne risque pas d'être commis sur Internet.

L'élément matériel de la troisième infraction est un acte à choix multiple : adapter ou reproduire ou divulguer une œuvre, ou exporter les copies d'une œuvre, représenter ou montrer ou divulguer une œuvre dans un lieu public

La tentative complète à ce crime est possible.

En ce qui concerne l'élément moral de cette infraction, celle-ci est intentionnelle.

L'élément d'illégalité est le manque de consentement de l'auteur de l'œuvre.

Les peines prévues sont soit alternatives soit cumulatives en fonction de l'importance du préjudice.

bbb. Les Atteintes aux droits moraux.

Les atteintes aux droits moraux sont régis par l'article 71 de la Loi[135].

« Celui qui, intentionnellement à l'encontre des dispositions de cette Loi ;

1. Publie ou représente une œuvre, qu'elle soit déjà publiée ou non, sans l'autorisation de son auteur ou du successeur de l'auteur,

2. Donne un nom à une œuvre ou à ses copies sans l'autorisation écrite de son auteur,

3. Montre l'œuvre d'autrui comme la sienne ou son œuvre comme celui d'autrui ou celui qui agit contrairement à l'article 15/2 du code,

4. Dans les cas cités aux articles 32, 33, 34, 35, 36, 37, 38,39 ne montre pas ses sources ou celui qui les montre fausses, insuffisantes et trompeuses,

5. Change une œuvre sans l'autorisation écrite de son auteur

Sera puni de deux à quatre ans de prisons ou de 50 milliards à 150 milliards de Lires Turques d'amende ou des deux en fonction de l'importance du préjudice. »

---

[135] Le texte en turc de l'article concerné de la Loi est ainsi :

"***Madde 71-*** *(Değişik:1. 11. 1983-2936/11)*

Bu Kanun hükümlerine aykırı olarak kasten: 1. Alenileşmiş olsun veya olmasın, eser sahibi veya halefinin yazılı izni olmadan bir eseri umuma arz eden veya yayımlayan, 2.Sahip veya halefinin yazılı izni olmadan, bir esere veya çoğaltılmış nüshalarına ad koyan, 3. Başkasının eserini kendi eseri veya kendisinin eserini başkasının eseri olarak gösteren veya 15'nci maddenin ikinci fıkrası hükmüne aykırı hareket eden, 4. 32, 33, 34, 35, 36, 37, 39 ve 40 ıncı maddelerdeki hallerde kaynak göstermeyen veya yanlış yahut kifayetsiz veya aldatıcı kaynak gösteren, 5. (Ek: 21.2.2001-4630/26) Eser sahibinin yazılı izni olmaksızın bir eseri değiştiren,

(Değişik: 3.3.2004-5101/17) Kişiler hakkında, iki yıldan dört yıla kadar hapis veya ellimilyar liradan yüzellimilyar liraya kadar ağır para cezasına veya zararın ağırlığı dikkate alınarak her ikisine birden hükmolunur." D'après www.ilesam.org.tr/telif.html (15.08.2004).

L' élément matériel de cette infraction est un acte à choix multiple : publier ou représenter une œuvre ou lui donner un nom , montrer l'œuvre d'autrui comme la sienne ou agir contrairement à l'article 15 /2 (ne pas faire figurer le nom de l'auteur sur les copies d'une œuvre des beaux arts ou ne pas indiquer sur une œuvre dérivée) ou dans les cas cités entre les articles 32 à 40 ne pas montrer ses sources, les montrer trompeuses, les montrer insuffisantes ou les montrer fausses ou changer une œuvre.

La tentative à ce crime n'est pas possible.

En tant qu'élément moral de l'infraction, celle-ci se commet nécessairement d'une manière intentionnelle.

L'élément d'illégalité est le manque d'autorisation écrite de l'auteur de l'œuvre.

Les peines prévues sont soit alternatives soit cumulatives en fonction de l'importance du préjudice.

b. Les atteintes au Droit des Marques sur Internet.

La Marque peut être définie brièvement comme « un signe sensible apposé sur un produit ou accompagnant un produit ou un service destiné à distinguer des produits similaires des concurrents. »[136]

Les atteintes au droit des marques sur Internet se manifeste de deux façons : premièrement par l'insertion de meta tags frauduleux, et deuxièmement par la contrefaçon de marque.

aa. L'insertion de « *meta tags* » frauduleux.

La publicité occupe une place très importante sur Internet.

De nouvelles formes de publicité intrinsèque ont apparu : il s'agit de s'aider des moteurs de recherche et annuaires. Les robots de moteurs de recherche travaille au niveau des mots clés choisi par le créateur du site Web ou directement sur tout ou une partie du texte de celle-ci.

---

[136] "A.Chavanne et J.J-Burst, *Droit de la Propriété Industrielle*,Dalloz,1998,no 857" d'après Pansier – Jez, op.cit, p.25.

Les « *meta tags* » sont des mots clés artificiellement ajouté au contenu de la page sans que cela soit perceptible par le visiteur mais influençant le comportement du robot qui analysera la page pour le référencer.

En soi, le procédé n'a rien d'illégal. Elle fausse le jeu normal de l'indexation des pages Web par le robot des moteurs de recherches, mais ce n'est pas en somme très critiquable comparé à des agissements beaucoup plus répréhensible.

Qu'en est il quand les « *meta tags* » utilisés sont des noms de marque ?

Voici quelques exemples de décisions américaines :

L'affaire « *İnsituform Technologies İnc.* » contre « *National Envirotech Group LLC.* » est l'une des plus connue à ce sujet[137].

« *İnsituform* » assigna « *National Envirotech* » en 1997, pour avoir utilisé leur nom et leur nom de produit « *İnsituform* » dans les meta tags.

Le mot « *İnsituform* » apparaissait dans les « *meta tags* », mais pas dans les pages Web. La seule raison plausible d'avoir utilisé le nom de marque dans les meta tags était de diriger les internautes vers le site de « *National Envirotech Group* ».

« *National Envirotech* » fût obligé par la Cour de faire disparaître l'expression « *İnsituform* » de ses meta tags.

Une autre affaire assez connue d'utilisation frauduleuse de « *meta tag* »est l'affaire « *Playboy* » contre Teri Welles .[138]

En l'espèce une ancienne salariée du magasine avait ouvert son propre site dans lequel était dissimulé le termes «*playboy* » et «*playmate* ». Mais cette fois-ci le juge décida que Welles avait des raisons légitimes d'utiliser ces expressions pour se décrire et cataloguer correctement son site Internet dans les moteurs de recherche et qu'elle n'avait pas l'intention de tromper les internautes et de fausser l'acheminement au site Web de « *Playboy* ».

Les « *meta tags* » frauduleux sont sans doute une forme relativement originale de contrefaçon de marque. D'autres modes de répression sont envisageables

---

[137]"İnstituform Technologies İnc.v. National Envirotech Group, L.L.C." d'après www.searchenginewatch.com/resources/metasuits.html. (09.12.2003).

[138] "Playboy vs. Terri Welles" d'apres www.searchenginewatch.com/resources/metasuits.html (09.12.2003).

telle la concurrence déloyale et l'action parasitaire. Il faut cependant que les conditions soient remplies, les sites doivent apparaître comme concurrent.

bb. La contrefaçon de marque par réservation de nom de domaine.

Le nom de domaine fait partie de la catégorie générale des identifiants nécessaire à toute activité commerciale.

En Droit commercial, les identifiants ou label peuvent faire l'objet d'une protection variée : la marque, le nom commercial et l'enseigne sont des identifiants juridiquement connu et protégé.

La tentation est grande d'identifier la marque protégée et le nom de domaine pour une entreprise. Pour beaucoup , la marque déposée est devenue nom de domaine : des Sociétés comme « *Peugeot* », « *Fiat* » , « *L'Oréal* » par exemple, ont construit des sites Internet en utilisant leur marque.

La règle générale dans l'attribution des noms de domaine est très simple : « Premier arrivé, premier servi »[139]. Est apparu alors très vite un problème de parasitisme du fait d'une course à l'enregistrement.

En effet le nom de domaine d'un site correspond à son adresse sur Internet et revêt une importance particulière. Il est alors intéressant de prendre un nom de site Web proche d'un nom de marque très connu ou l'enregistrement d'un patronyme, d'un lieu géographique.

On a donc vu un véritable trafic international des noms de domaine, des individus revendant les noms qu'ils avaient pensés à enregistrer plus rapidement que les personnes concernées plus légitimement.

Il existe donc des spécialistes de dépôts massifs de noms de domaine voisins de marques ou de dénominations existantes.

Ces exercices frauduleuses sont dénommées par la pratique de « *cybersquattage* » lorsque l'utilisateur du nom de domaine a déposé un nom de domaine dont il sait l'intérêt pour une entreprise et tente de le monnayer par la suite. Il est à noter qu'il faut souvent payer le « *cybersquatter* » pour qu'il parte.

Au niveau mondial c'est l'organisation mondiale de la propriété intellectuelle qui traite les conflits contre les cybersquatters.

---

[139] Pansier-Jez, Op.cit, p.27.

Elle a ordonnée en 2001 le transfert de nom de domaine « *TF1.net* » à la société française de télévision *TF1*.[140]

En France, une autorité d'enregistrement chargée de l'attribution des noms de domaines a été fondée : L'Association Française pour le Nommage İnternet en Coopération (AFNİC) opérée par l'İnstitut National pour la Recherche en İnformatique et en Automatique (İNRİA). Cet organisme a élaboré une « convention de nommage »[141] fixant les critères pour l'attribution du nom de domaine. Ainsi lorsque le nom est un nom de marque, le certificat d'enregistrement a l'İNPİ et son numéro doivent être fournis.

Les Etats-Unis ont introduit au début de l'année 2000 une législation spécifique ; la Loi « *Anticybersquatting Consumer Protection Act* » dite ACPA : est civilement responsable envers le titulaire d'une marque toute personne qui de mauvaise foi et avec l'intention d'en tirer un profit de ce dépôt, enregistre, vend ou utilise un nom de domaine qui à la date de son enregistrement, soit est identique ou similaire à une fabrique distinctive , soit opère une dilution de la marque, soit enfin consiste en certaines marques ou certains mots ou noms protégés par la Loi.

Dans un arrêt du 8 janvier[142], la cour fédérale d'appel a utilisé pour la première fois ce texte. En l'espèce, les opérateurs d'un moteur de recherche ayant déposé le nom de domaine « *northernlight.com* » et la marque « *Northern Light* » se sont opposé à un cybersquatter ayant déposé le nom de domaine « *Northernlights.com* ». Les demandeurs victimes avaient agi en contrefaçon de marque et concurrence déloyale par « *cybersquatting* ». İls obtinrent au premier degré l'interdiction au cybersquatter de l'utilisation du nom de domaine. La Cour d'appel reconnut que le défendeur était de mauvaise foi.

De ces constats, nous pouvons en déduire pour conclusion que la marque est très attractive du fait lorsqu'il s'agit de défendre un nom de domaine ou de s'opposer à un nom de domaine incorrectement attribué. Dans ces cas, en Turquie, seul le droit des marques ou le droit commun de la concurrence déloyale peuvent être utilisé. Or le droit des marques puisant sa source du Décret Loi no 556 sur les marques en Turquie, est plus certaine que l'action en concurrence déloyale fondée sur le texte général du Code Commerciale (article 57).

---

[140] Pansier – Jez,Op.cit, p.28.

[141] disponible sur internet à l'adresse www.nic.fr/procedures.nommage.htm.

[142] Pansier – Jez, Op.cit, p.29.

cc. La Répression

La définition de la marque en Droit Turc est la suivante :

D'après le Décret Loi no 556 art 5 : « A condition que la marque permettent de différencier les produits et les services d'une Entreprise de ceux d'une entreprise concurrente,

Elle est formée des mots y compris les prénoms, les noms, des formes, des lettres, des chiffres, des images permettant de visualiser la forme des produits ou de leur emballage, et des signes pouvant être reproduit et publié par l'intermédiaire de l'imprimerie. »

Dans la mesure où les noms de domaine sont formés à partir mots et des noms ou prénoms, ils peuvent être considérés comme des signes de marque au sens de la définition.

Par conséquent celui qui prend un nom de domaine proche du nom d'une marque enregistrée pour commercialiser la même sorte de produit, sera considéré comme avoir violé les droits découlant de la Marque au sens de l'article 5.

L'utilisation d'une marque en tant que nom de domaine entre dans le champ d'application de l'art 61/b du Décret –Loi no : 556 selon lequel « imiter la marque en utilisant le nom de la marque enregistrée ou un nom lui ressemblant au point de ne pas être différencié, sans l'autorisation de son titulaire » constitue un crime puni de deux à quatre ans de prisons et de 600 millions a un milliard de Lires Turque d'amende, de la clôture de l'entreprise imitante au moins pendant un an et son interdiction du commerce pendant la même durée.

Cette infraction est forcément commise intentionnellement. Une intention générale suffit.

Le Décret Loi a cependant instauré une condition préalable à la poursuite : le titulaire du marque doit porter plainte auprès du Procureur de la République, dans les deux ans suivant son appréhension de la violation ou de l'identité de l'auteur de la violation.

2. Les atteintes aux biens matériels : La Fraude.

L'industrie informatique s'est hissée en quelques années au troisième rang des secteurs les rentables, juste derrière la drogue et le pétrole...[143]

Le développement de la nouvelle pierre angulaire de l'économie a été cimenté à coup d'extorsion, d'appropriation abusive et de fraude.

Les autorités américaines sont perplexes : ils ont recensé le 12 septembre 2002, 100.000 transactions illicites initiés auprès d'une vingtaine de sites de commerce électronique, dont prés de 60.000 ont été acceptés[144]. Certes, il s'agit pour la plupart des sites mineurs et les montants de ces échanges ne dépassaient pas 5€. Pour les autorités bancaires, il s'agit d'une arnaque à plus grande échelle : les pirates pourraient disposer d'une source encore plus importante de coordonnées bancaires dérobées et aurait simplement voulu vérifier la validité, peut être avant d'acheter le reste.[145]

Nous verrons dans cette partie les différents types de fraude et leur répression en Turquie.

a. Les différents types de fraude.

Le type le plus fréquent de ce crime est certes la fraude assistée par ordinateur. Parmi les faits d'arme les plus célèbres, le détournement par des pirates de plus de soixante dix millions de dollars de la « *First National Bank of Chicago* » peut être cité.[146]

Le « *carding* » est un autre type de fraude : c'est le détournement de moyen de paiement électronique. Le « *carding* » est le nom générique qui recouvre l'ensemble des délits relatifs aux fraudes basées sur l'utilisation frauduleuse des nouvelles technologies. Le « *carding* » consiste essentiellement à générer à l'aide d'un logiciel extrêmement facile à trouver sur İnternet, de vraix ou faux numéros de cartes bancaires, ainsi que des vrais et fausses dates de validité.

---

[143] www.indexel.net/1_20_2931_/alerte_a_l'_escroquerie.htm (02.09.2004).
[144] İbid.
[145] İbid.

[146] Châtelain – Roche , Op.cit,p.116.

Une affaire relativement récente a ainsi provoqué un préjudice financier très important consécutif à la commande de microprocesseurs de type Pentium III 600 pour un montant cumulé de 60980 Euros, au détriment d'une Entreprise française de vente par correspondance sur Internet. Si les commandes ont été passées à l'aide de trois cartes bancaires différentes, les livraisons elles, ont été effectuées à une seule et même adresse à Londres.[147]

Le « *skimming* » est une autre forme fréquent de fraude : Parmi les cyberdélits les plus visibles par le grand public les fraudes à cartes bancaires occupent une place particulièrement importante. Les utilisations de codes secrets, les paiements des services de téléchargement de logiciel en ligne, les connexions sur des serveurs pornographiques, les achats de matériels auprès des sites marchands, sont tous regroupés sous le terme général de « *skimming* ».[148]

Le «*skimmer* » est un appareil conçu pour lire les informations stockées sur les bandes magnétiques des cartes de crédit. Aussi le skimmer dont l'utilisation première est tout à fait légale, enregistre l'information de la carte de crédit stockée sur la bande magnétique (information qui permet de faire des achats illégaux ou de créer de nouvelles cartes de crédits).

Une autre forme de fraude consiste à garder un dispositif supplémentaire de « *skimming* » dans une mémoire à côté de la machine officielle de paiement par carte. La carte est d'abord lue par cette première machine pour approbation d'achat puis par le dispositif illégal de « *skimming* » afin de copier l'information contenue sur la bande magnétique. Une complicité avec un employé est nécessaire. Ce type de fraude s'observe particulièrement dans les entreprises où la rotation des employés est importante (dans les restaurants ou les stations d'essence). Pour tenter de réduire ce type de fraude de nombreux établissements bancaires investissent dans la recherche et le développement à l'exemple de « *Mastercard İnternational*» qui travaille actuellement avec « *Mag Tek İnc.* », un fournisseur international majeur des technologies et des produits de lecteurs de cartes.

Enfin le «*phishing* »[149] est la forme de fraude la plus récente : c'est une forme de fraude en ligne consistant à imiter le site Web d'une institution bancaire pour inciter le visiteur à dévoiler les informations confidentielles sur ses comptes

---

[147] İbid, p 112.
[148] İbid,p.113.
[149] www.infodunet.com/news/3465-phishing.html. (02.09.2004).

comme par exemple les coordonnées détaillées de sa carte de crédit, y compris son code secret.

Les chercheurs de « *Sophos* » estiment que des centaines de milliers d'e-mails de «*phishing* » sont envoyés chaque jour via Internet tous conçu pour détourner l'argent de l'utilisateur sans méfiance.

Jusqu'à présent ce type d'attaque était surtout le fait de groupes criminels organisés, mais avec des outils désormais accessibles sur le net, même pour les amateurs cette inquiétante tendance ne peut que s'amplifier.

b.La Répression

Le Code Pénal Turc régit la fraude informatique dans son article 525 b-2. La disposition est la suivante : « celui qui utilise une système automatique d'informatisation des données afin de procurer illégalement un bénéfice à son compte ou à celui d'autrui sera puni de 1 à 5 ans de prison et de à 20 millions de Lires turques d'amende. »

Le sujet du crime est un bénéfice illégal.

L'élément matériel du crime est une conduite est à multiple choix : l'acte pour réaliser le crime n'a pas été précisé dans la disposition. Cela veut dire que n'importe quel acte permettant d'atteindre le but est valable. Néanmoins, la seule condition est de se servir comme support d'un système automatique d'informatisation des données.

Le résultat du crime est l'obtention d'un bénéfice illégale pour son propre compte ou celui d'autrui.

Toute sorte de tentative (complète et incomplète) est possible.

En tant que élément moral du crime : une intention particulière est requise. L'auteur doit porter l'intention de produire un bénéfice pour son propre compte ou pour celui d'autrui.

Il faut noter que la fraude informatique a été reprise dans la Loi portant sur le Nouveau Code Pénal dans l'article 244-3:

La disposition est comme la suivante [150]:

---

[150] Le texte en turc de l'article concerné est ainsi :

"*Sistemi engelleme, bozma, verileri yok etme veya değiştirme*

« Celui qui procure un intérêt illégitime pour son propre compte ou pour celui d'autrui en commettant les actes définis dans les paragraphes précédents, sans que ceux-ci ne forment un autre crime, sera puni de deux à six ans de prison et de peine pécuniaire judiciaire de 5000 jours. »

Tout d'abord, les actes définis dans les paragraphes précédents sont, l'empêchement du fonctionnement d'un système informatique ; sa mise en panne, l'emplacement illégal de données à l'intérieur d'un système informatique, l'envoi des données existantes vers un autre système informatique, la mise en état d'inaccessibilité certaines données, leur changement et leur destruction..

En ce qui concerne l'élément matériel du crime ; contrairement, à l'article 525-b/2 du code pénal, les actes sont précisés. Le premier paragraphe de l'article énumère les actes possibles pour la réalisation du crime. İci aussi nous somme face à un crime dont les actes sont à multiple choix. Il suffit que l'un d'entre eux soit réalisé. La seule condition est de se servir d'un système informatique.

Toute sorte de tentative (complète ou incomplète) est possible.

Le résultat du crime est l'obtention d'un bénéfice ou d'un intérêt illégale.

Le crime doit être commis avec une intention particulière celui de procurer un bénéfice pour son propre compte ou pour celui d'autrui.

B. Les crimes de nature éditoriale s'attaquant aux personnes

Parmi ces crimes, nous pouvons citer les délits allant à l' encontre de la protection du mineur, les atteintes à la vie privée, et les infractions de Presse

---

MADDE 244- (...)

(3) Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adli para cezasına hükmolunur." D'apres www.tcktasarisi.org. (10.09.2004)

1. Les Délits allant à l'encontre de la protection du mineur.

a. La protection du mineur des publications obscènes.

L'Internet constitue un danger à la morale du mineur dans la mesure où il permet la divulgation des publications obscènes tels les publications pornographiques ou incitant à la violence ou à la haine raciale.

Certes la protection de la moralité du mineur est avant tout un devoir parentale, mais sa mise en œuvre parait difficile face à l'immensité de la ressource et à l'extrême diversité des contenus circulant sur le réseau.

Cependant la mise en œuvre d'un contrôle familial semble devenir possible avec l'apparition de logiciel et de société de service assurant le filtrage des sites ou informations directement consultables par un mineur connecté au réseau. C'est le cas par exemple, du fournisseur d'accès « *Superonline* » en Turquie, commercialisant aux familles un logiciel de filtrage des informations visant à protéger les mineurs des sites sur İnternet dont le contenu risquent d'être obscène ou violent. En France, ce sont les logiciels tel que « *Net Nanny* » ou « *Cybersitter* »[151] qui assurent ces fonctions.

Cependant, le recours à ces options techniques, bien que encouragé par les partisans de l'autorégulation de l'İnternet et, est loin d'assurer une protection optimale.

Il semble nécessaire d'apporter un soutien à ce procédé de filtrage avec des dispositions légales.

En Turquie, nous disposons d'une Loi datant du 21/6/1927 et ayant été sujets à de sérieux amendements en 1986, sur « La Protection du Mineur des Publications Obscènes »[152]. Son but, comme son nom l'entend si bien, est de protéger le mineur de publications susceptibles de porter atteinte à leur morale. Dans le premier article de cette Loi, son champ d'application est défini de la manière suivante :[153] « Les publications périodiques et les autres œuvres imprimés n'entrant

---

[151] Pansier- Jez,Op.cit ,p.83

[152] En Turc : *1117 sayılı "Küçüklerin Muzır Neşriyattan Korunma Kanunu."*

[153] Le texte de l'article concerné en turc est : *Madde 1 - (Değişik: 6/3/1986 - 3266/1 md.) 18 yaşından küçüklerin maneviyatı üzerinde muzır tesir yapacağı anlaşılan*

pas dans la définition de publications périodiques, susceptibles de porter atteinte à la moralité du mineur seront assujettis aux limitations prévues telles dans les articles suivants. »

Comme nous pouvons en déduire du texte de l'article, cette Loi n'est pas applicable à l'İnternet puisce que son champ d'application ne s'étend qu'aux publications périodiques et non périodiques imprimés. Dans la mesure où la divulgation d'informations obscènes n'est pas imprimée et revendues par la suite cette Loi ne pourra pas être appliquée.

L'ancien Code pénal turc aussi ne prévoyait pas de dispositions réglementant les attaques à la moralité du mineur. Le nouveau Code pénal turc en prévoit une.

L'article 226 sur le Nouveau Code Pénal Turc dispose [154] :

« a. Celui qui donne des images obscènes ou des produits contenant des textes ou des paroles obscènes ou qui montre, lit ou fait lire ou fait écouter le contenu de ces même produits à un mineur

b. Celui qui montre, expose, lit, fait lire le contenu des produits obscènes dans des lieux publics où les enfants peuvent aller,

c. Celui qui commercialise ou qui loue ces produits de manière à percevoir leur contenu,

d. Celui qui commercialise, ou vend ou loue les produits à contenus obscènes en dehors des lieux spécialisés à leur vente,

---

mevkute ve mevkute tanımına girmeyen diğer basılmış eserler aşağıdaki maddeler-de gösterilen sınırlamalara tabi tutulur. (1) d'apres www.hukuki.net/mevzuat (05/09/2004).

[154]Le texte en turc de l'article concerné est comme le suivant :

" MADDE 226- (1) a) Bir çocuğa müstehcen görüntü, yazı veya sözleri içeren ürünleri veren ya da bunların içeriğini gösteren, okuyan, okutan veya dinleten,

b) Bunların içeriklerini çocukların girebileceği veya görebileceği yerlerde ya da alenen gösteren, görülebilecek şekilde sergileyen, okuyan, okutan, söyleyen, söyleten,

c) Bu ürünleri, içeriğine vakıf olunabilecek şekilde satışa veya kiraya arzeden,

d) Bu ürünleri, bunların satışına mahsus alışveriş yerleri dışında, satışa arzeden, satan veya kiraya veren,

e) Bu ürünleri, sair mal veya hizmet satışları yanında veya dolayısıyla bedelsiz olarak veren veya dağıtan,

f) Bu ürünlerin reklamını yapan,

kişi, altı aydan iki yıla kadar hapis ve adli para cezası ile cezalandırılır." D'apres www.tcktasarisi.org (10.09.2004).

e. Celui qui donne ou distribue gratuitement ces produits indirectement ou a côtés d'autres services et de produits.

f. Celui qui fait la publicité de ces produits,

Sera punis de six mois à deux ans de prisons et de peine pécuniaire judiciaire. »

Il s'agit d'une infraction dont les actes sont à choix multiples :

Ces actes sont décrits dans les cinq alinéas de l'article. Il suffit d'en commettre un afin que le crime soit réalisé.

Dans tous les cas une intention générale semble suffire.

La tentative ce crime est possible.

Cette disposition peut parfaitement s'appliquer à l'Internet étant donné qu'une précision sur les supports n'a pas été faite.

Il faut d'autre part préciser qu'une peine plus lourde est prévue dans le cinquième paragraphe de ce même article :

« Celui qui publie ou sert d'intermédiaire à la publication par la voie de la presse ou assure que les mineurs voient, écoute ou lit, des produits prévus dans le troisième et quatrième paragraphe, sera punis de six ans à 10 ans de prisons et jusqu'à 5000 jours de peine pécuniaire judiciaire. »

Les produits qui sont le sujet du crime et qui sont décrit dans le troisième et quatrième paragraphe de l'article sont, des produits qui mettent en scène des enfants engagés dans des activités sexuelles, ou des scènes de violence.

C'est la raison pour laquelle la peine prévue est plus lourde ici.

Là aussi une intention générale semble être suffisante.

b. La Cyber pédophilie

Le Conseil d'Europe qualifie la pornographie enfantine en termes généraux comme « tout matériel pornographique qui décrit ou représente visuellement un enfant réel impliqué ou se livrant à un comportement sexuel explicite; ou une personne réelle apparaissant comme étant un enfant impliqué ou se livrant au comportement mentionné ci-dessus; ou des images réalistes d'un enfant

non existant impliqué ou se livrant au comportement mentionné ci-dessus »[155] L'Organisation Internationale de la Police criminelle (Interpol) définit la pornographie enfantine comme la « Représentation audiovisuelle de l'exploitation sexuelle d'un enfant, qui met l'accent sur le comportement sexuel de l'enfant ou sur ses organes génitaux. ».[156]

L'Internet a donné à la pédophilie une dimension différente en lui offrant des moyens inégalés. L'internet a favorisé la diffusion du message pédophile plus que ne l'avait fait aucun médium auparavant, les réseaux de trafiquants devenant internationaux. [157]

La pédophilie est la démonstration caricaturale des abus auxquels peut conduire un usage trop libre de l'Internet.

En dehors du net, les pédophiles se heurtent à un mur de honte et la seule possibilité pour eux d'assouvir leur passion immorale est de se constituer en réseau.

En réponse, de nombreuses organisations de lutte contre la pédophilie se sont installés sur le Net et recensent minutieusement toutes les informations sur les individus susceptibles de s'adonner à ces activités[158]. L'Association Américaine Pedowatch (constituée pour régler le problème de surveillance de l'Internet) a recensé au Japon par exemple 1200 à 1300 sites pornographiques dont une majorité montre des activités sexuels avec des mineurs.

aa. Comment la pédophilie se répand sur Internet ?

Un enthousiaste de la pornographie enfantine ne peut s'exposer dans des sites fixés.

Les adhérents à cette sous culture sont obligés d'utiliser une variété d'alternatives pour se dissimuler.

Ces alternatives peuvent être regroupés sous quatre titres[159] :

---

[155] Indragandhi Balassoupramaniane, "La pornographie enfantine, la réponse du Conseil d'Europe" d'apres www.barreau.qc.ca/journal/frameset.asp?article=/journal/vol35/no 4/droitcompare.(17.08.2004).

[156] "la pornographie infantile" http://users.swing.be/criminologie/contenus/ch2/pornodown.htm. (17.08.2004).

[157] Philip Jenkins, Beyond Tolerance : Child Pornography on The Net, New York, University Press , 2001, p.5.

[158] www.pedowatch.org/index.html.

[159] Yaman Akdeniz, Sex on the Net : The Dilemna of Policing Cyberspace, United Kingdom – Reading, South Street Press; 1999, p.10.

- les « *Newsgroups* »
- les bulletins d'histoire
- les « *bulletins boards* »
- les groupes clos

Les « *Newsgroups* » sont en général des groupes binaires, c'est-à-dire qui permettent l'échange de photos et d'images. Ils constituent un plateforme d'échange à la pédo-pornographie. Le plus connu de ces groupes est le « pictures.erotica.preteen. (abpept) »

Les bulletins d'histoire sont constitués d'histoires et de phantasmes s'adressant aux pédophiles.

Les « *bulletin boards* » sont des sites ouverts. Ils sont les centres de commandes du trafic entier de la pédopornographie. C'est ici que les adhérents s'échangent les adresses des sites. Quelques sites du « bulletin boards » permettent aussi la discussion. Ces sites offrent une source extrêmement riche aux membres de cette sous culture.

Les groupes clos ou réseaux électroniques fermés sont extrêmement difficile à pénétrer. Les utilisateurs ont des talents très développés en technologie. Ils sont constitués d'un cercle d'individus qui se connaissent très bien et ayant prouvé leur confiance mutuelle sur une période de 5 à 6 ans. Ces personnes ne souhaitent pas de nouveaux contacts. Elles disposent de plusieurs méthodes clandestines de distribution et elles poursuivent de très près les progrès technologiques pouvant protéger leur sécurité et leur secret.[160]

bb. La répression de la cyber pédophilie en droit comparé.[161]

La pédo-pornographie est régie en France par l'article 227-23 du code pénal français, en Angleterre par la Loi de 1978 et de 1988, en Italie par l'article 600 ter et quarter du code pénal italien, en Espagne par l'article 189-1 du nouveau code pénal, en Autriche par l'article 207 du code pénal, en Allemagne par l'article 184-3 du code pénal. Ce sont toutes des dispositions spécifiques.

En Angleterre, en Italie, en Autriche et en Allemagne, même la possession (sur n'importe quel support) d'images d'enfants engagés dans des activités sexuelles est réprimée.

---

[160] Jenkins,op.cit , p.58.
[161] http:/users.swing.be/criminologie/contenus/ch3/repression.htm (17.08.2004).

La peine pour la possession est de 5000 Sterlin d'amende en Angleterre, de 3 ans de prisons ou de minimum 3 millions de lires d'amende en Italie, de six mois de prison en Autriche, d'un an de prison en Allemagne.

La peine pour la diffusion d'image est de 5 ans de prisons et de 500.000. Francs en France, de 18 mois de prison en Angleterre, de un a cinq ans de prisons et de 50 a 100 millions de Lires, d'un de prison en Autriche, et de trois mois a cinq ans de prison en Allemagne. En Espagne seule la reproduction (et non pas la diffusion) est punie de un a trois ans de prison.

cc. La répression en Turquie

La Turquie ne disposait pas de législation spécifique jusqu'à la promulgation du nouveau code pénal, concernant la diffusion et la possession d'objets mettant en scène la pornographie enfantine.

Pour cela nous devions nous référer aux dispositions générales du Code Pénal pour réprimer ce type d'acte criminel.

Selon l'article 426 du code pénal,

« 1. Celui qui publie, distribue, vend, ou fait publier, distribuer, vendre, ou celui qui dans l'intention de commercialiser ou de distribuer ou d'imprimer ou de publier, dessine, peint, produit, imprime, multiplie, dicte ou fait dessiner-peindre-produire-imprimer-multiplier-dicter : celui qui importe ou exporte ou transporte à l'intérieur du territoire turc d'un lieu à un autre ; celui qui réalise un traitement quelconque sur, ou celui qui dans l'intention de faciliter la commercialisation commet ces acte ; ou celui qui procure ou fait procurer ou affirme qu'il peut procurer un livre, un journal, une brochure, une revue, une feuille, un article, une annonce, un image, une peinture, des disques, une affiche, une pancarte, une télévision , une cassette audio, un photographe, ou d'autres outils et moyen d'expression,

2. Celui qui représente ou fait représenter dans les milieux publics, à la télévision ou la radio ou au cinéma ou au théâtre des œuvres,

3. Celui qui dans un lieu public réalise une allocution,

Qui vont à l' encontre de la pudeur et de la malséance du public ou qui abuse et excite son désir sexuel contrairement au moral public,

Sera puni de 6 à 30 millions Lires Turques d'amende.

Au cas où ces actes sont réalisé par l'intermédiaire des publications à durée déterminée décrie à l'article 3 de la Loi no 5680 sur la Presse, les auteurs et les propriétaires seront punis d'une amende dont la valeur sera évaluée par rapport à la moyenne de la vente effective durant le mois précédent, si la durée de la publication est inférieur à un mois,

Au cas où cette durée est supérieure à un mois, la valeur de l'amende pourra être évalué jusqu'à 90 % de la valeur de la vente totale du mois précédent.

Dans les deux cas l'amende ne pourrait être inférieur à 30 millions.

Les directeurs responsables de ces publications à durée déterminée seront punis de la moitié de la peine attribuée aux propriétaires. »

Cet article pourra être appliqué à la pornographie dans la mesure où le législateur a évité de faire une énumération exhaustive des supports de publications, en finissant la liste par « autre moyen de publication ». Il est certain que l'İnternet est un outil de publication.

Il est regrettable que la pornographie enfantine n'ait pas été le sujet d'une législation spécifique car la répression prévue dans cette disposition générale est loin d'être dissuasive. Alors que dans les pays de l'Union Européenne, ce crime est puni jusqu'à 5 ans de prison (İtalie et Allemagne), en Turquie qu'une peine pécuniaire est prévue.

Le sujet du crime prévu dans l'article 426 du Code Pénal, est les images et les représentations obscènes.

L'élément matériel de cette infraction est des actes à choix multiples et sont énumérés dans le texte de l'article. Voici quelques une de ces actes : publier, distribuer, vendre, imprimer, produire, peindre, multiplier (...) des images ou des réalisations à caractères pornographiques et obscènes.

Le résultat de l'acte est simultané avec sa réalisation.

Une intention générale, pour la réalisation, est suffisante.

En tant qu'élément illégalité, l'acte constituant le crime doit aller à l'encontre du moral public.

La tentative incomplète et la tentative complète sont possibles.

Bien qu'il n'y ait pas de dispositions particulières prévues dans l'ancien Code pénal turc, la Loi sur le nouveau Code pénal en prévoie une.

C'est l'article 226/3 du nouveau Code pénal. Cet article régit les publications obscènes et elle prévoit dans son troisième paragraphe une peine pour la pornographie enfantine.

Le troisième paragraphe concernant notre sujet est ainsi :

« Celui qui utilise les enfants dans la production d'images de textes ou de paroles obscènes sera punis de 5 à 10 ans de prisons et jusqu'à 5000 jours de peines pécuniaires judiciaire. Celui qui fait pénétrer ces produits dans le pays, les multiplie, les vend, les transporte, les emmagasine, les exporte, les dispose ou les met à la disposition d'autrui sera puni de 2 à 5 ans de prison et jusqu'à 5000 jours de peines pécuniaires judiciaires. »[162]

---

[162] Le texte en turc de l'article concerné est comme le suivant

"Müstehcenlik

MADDE 226- (1) a) Bir çocuğa müstehcen görüntü, yazı veya sözleri içeren ürünleri veren ya da bunların içeriğini gösteren, okuyan, okutan veya dinleten,

b) Bunların içeriklerini çocukların girebileceği veya görebileceği yerlerde ya da alenen gösteren, görülebilecek şekilde sergileyen, okuyan, okutan, söyleyen, söyleten,

c) Bu ürünleri, içeriğine vakıf olunabilecek şekilde satışa veya kiraya arzeden,

d) Bu ürünleri, bunların satışına mahsus alışveriş yerleri dışında, satışa arzeden, satan veya kiraya veren,

e) Bu ürünleri, sair mal veya hizmet satışları yanında veya dolayısıyla bedelsiz olarak veren veya dağıtan,

f) Bu ürünlerin reklamını yapan,

kişi, altı aydan iki yıla kadar hapis ve adli para cezası ile cezalandırılır.

(2) Müstehcen görüntü, yazı veya sözleri basın ve yayın yolu ile yayınlayan veya yayınlanmasına aracılık eden kişi altı aydan üç yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır.

(3) Müstehcen görüntü, yazı veya sözleri içeren ürünlerin üretiminde çocukları kullanan kişi, beş yıldan on yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır. Bu ürünleri ülkeye sokan, çoğaltan, satışa arzeden, satan, nakleden, depolayan, ihraç eden, bulunduran ya da başkalarının kullanımına sunan kişi, iki yıldan beş yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır.

(4) Şiddet kullanılarak, hayvanlarla, ölmüş insan bedeni üzerinde veya doğal olmayan yoldan yapılan cinsel davranışlara ilişkin yazı, ses veya görüntüleri içeren ürünleri üreten, ülkeye sokan, satışa arzeden, satan, nakleden, depolayan, başkalarının kullanımına sunan veya bulunduran kişi, bir yıldan dört yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır.

(5) Üç ve dördüncü fıkralardaki ürünlerin içeriğini basın ve yayın yolu ile yayınlayan veya yayınlanmasına aracılık eden ya da çocukların görmesini, dinlemesini veya okumasını sağlayan kişi, altı yıldan on yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır.

(6) Bu suçlardan dolayı, tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur.

(7) Bu madde hükümleri, bilimsel eserlerle; üçüncü fıkra hariç olmak ve çocuklara ulaşması engellenmek koşuluyla, sanatsal ve edebi değeri olan eserler hakkında uygulanmaz."

D'après www.tcktasarisi.org (10.09.2004).

Ainsi pour la première fois en Turquie, la production et la diffusion et même la possession d'images obscènes mettant en scènes des enfants sont incriminées et est punie pour la première de 5 à 10 ans de prisons et jusqu'à 5000 jours de peines pécuniaires judiciaires, et pour la deuxième et la troisième de deux à cinq ans de prison et de 5000 jours de peine pécuniaire judiciaire.

La possession et la diffusion d'image obscènes sont traitées dans une même infraction.

Le paragraphe en question contient donc deux infractions.

L'élément matériel de la première infraction est le fait de produire des images obscènes mettant en scène des enfants.

Le résultat de l'acte et l'acte sont simultanés.

Cette infraction est forcément commise intentionnellement. Une intention générale est suffisante.

La tentative complète et incomplète à cette infraction est possible.

En tant qu'élément matériel de la deuxième infraction décrite dans ce même paragraphe, les actes permettant la réalisation du crime sont les faits de faire pénétrer les produits obscènes en Turquie, de les distribuer, de les emmagasiner, de les exporter, de les disposer, de les mettre à la disposition d'autrui.

Ce crime aussi est intentionnel.

Toute sorte de tentative à ce crime, est possible.

2. Les atteintes à l'intimité de la vie privée sur Internet.

L'anonymat sur İnternet est un grand mythe[163]. La réalité est autre. L'anonymat n'est pas la règle sur İnternet et l'absence de trace l'est encore moins. İl est possible d'être sinon espionné, du moins surveillé, peut être pas étroitement, mais suffisamment pour qu'un marché des outils de surveillance existe et que cette surveillance puisse être le fait d'acteurs de nature très diverses...

Se pose dés lors le problème de la protection de la vie privée.

---

[163] Durmuş Tezcan, "İnternet karşısında özel hayatın korunması"
Dokuz Eylül Üniversitesi 21-22 Mayıs Uluslararası İnternet Hukuku Sempozyumu, İzmir, Dokuz Eylül Üniversitesi Yayınları, 2002, p.535.

La vie privée peut être définie comme les faits d'une personne que pas tout le monde ne sait et dont la connaissance peut être acquérie à l'aide d'une recherche spécifique.[164]

Les moyens de recherches spécifiques sont abondants sur İnternet à tel point qu'il devient parfois inéluctable de dévoiler sa vie privée.

a) Les moyens de violation.

İl n'est pas possible d'élaborer une liste exhaustive des moyens de violation. Ces derniers peuvent varier en fonction des changements et des innovations technologiques. Les moyens de violation présents sont les suivants.

aa. Le courrier électronique

İl est possible de porter atteinte à l'honneur et à la dignité, à la vie privée et au secret, à l'image, au nom, aux droits de personnalités d'une personne par l'intermédiaire de l'e-mail.

Il est possible d'envoyer en compagnie du courrier électronique un virus qui puisse rendre l'ordinateur du récepteur inutilisable ou transférer les données qui y sont enregistrées vers un autre ordinateur. Dans tous les cas, l'atteinte à la vie privée sera accomplie. Par exemple, un chef de parti politique en Turquie avait réussi à intercepter les courriers électroniques de Karen Fogg, représentante de l'union Européenne en Turquie et il les avait publié.

L'envoi de courrier électronique contenant des fausses nouvelles sur une personnes ou des nouvelles susceptibles de ridiculiser celle-ci, ou décelant les secrets de sa vie à des tiers constituera une violation de la vie privée.

Le problème avec les courriers électroniques est la détermination de la personne émettrice car il est possible de s'approprier des adresses e-mail avec des pseudonymes, il serait alors impossible de découvrir l'émetteur du courrier.

bb. Les Sites Web.

La violation du droit à la vie privée par l'intermédiaire des sites Web est très fréquente. İl est possible par exemple de dévoiler les secrets d'une personne, de transmettre les nouvelles concernant sa vie de couple, d'attaquer son honneur et sa

[164]Çetin Özek, Türk Basın Hukuku, İstanbul,1978, p.259.

dignité, de le ridiculiser et de se moquer, de publier son image sans son autorisation sur un site web.

cc. Les banques de données électroniques

La formation de banques de données surtout par des personnes morales privées comme les banques (souvent pour accorder des crédits) et les grandes entreprises (pour le recrutement de leur personnel) est particulièrement menaçante pour la protection de la vie privée. Le prénom, le nom, l'âge, le sexe, le statut social, la famille, la profession, le revenu, ses dettes, ses maladies et des renseignements semblables forment les données privées d'un individu.[165]

Ces renseignements peuvent être rassemblés sur Internet par de différentes manières : par exemple en s'enregistrant auprès d'un fournisseur d'accès à l'Internet pour obtenir une adresse et un compte e-mail ou pour bénéficier des services de banques électroniques. Ces renseignements sont souvent donnés par la personne concernée elle-même. Tout de même ce consentement ne comprend pas leurs transmissions à un tiers. Celui qui agit en dehors de ce consentement provoquera la violation de la vie privée.

dd. Les courriers non sollicités : les « *Spam* ».[166]

Les spammeurs n'hésitent pas à récolter les adresses e-mail (une donnée personnelle nominative et privée) sur les « *Newsgroups* », les espaces de discussions, les listes de diffusions, les annuaires diffusés sur les sites Web et créer d'énormes listes d' « e-mail » qu'ils utilisent pour leur campagne de publicité, mais aussi pour les revendre à d'autres spammeurs. En cela, ils violent aussi en permanence ce qu'on appelle la « Netiquette » qui est un ensemble de règles établie pour vivre un Internet éthique et respectueux.

ee. Les « *Cookies* »

La plupart du temps les serveurs proposent aux internautes de placer un « *cookie* » dont ils ignorent le terme et ils cliquent sur « O.K » sans se préoccuper de son devenir.

---

[165] Tezcan,op.cit, p.535.
[166] "Pourquoi Lutter contre le Spam" www.caspam.org/spam.html (01.09.2004).

Ce « *cookie* » est en effet un fichier stocké sur le disque qui permettra au serveur de les reconnaître la prochaine fois qu'ils reviendront sur le site de telle façon à connaître leurs préférences et pour leur éviter de les ressaisir. [167]

Le problème de ces « *cookies* » est qu'ils contiennent des informations sur les internautes.

En effet lorsqu'ils se connectent à un site, celui-ci va leur poser quelques questions afin de dresser leur profil.[168]

En formant une liste de profils dessinées par les interrogations effectués sur les sites Web ou les Newsgroup sur Internet ou en interrogeant des listes de classifiés par matière dans lesquelles ils figurent, la détermination de leur personnalité va devenir possible : « un avocat, mâle, taille moyenne, militant d'extrême gauche, passionné de Frank Sinatra, spécialiste du droit du travail, très endetté, amateur des sites de charmes. ». Au fur et à mesure l'empreinte de leur préférence affinera le portrait. Les sites dans lesquelles il figure sera revendue très chers à des commerçants et peut être parfois à des ministres[169] et autres censeurs ou à leur employeurs. Les Etats répressifs assurent grâce aux « *cookies* » ou autres techniques similaires, la surveillance de leurs éléments subversifs. Les entreprises ne conserveront que leurs employés modèles.

b) La répression.

En Droit Turc, le droit à la protection de l'intimité de la vie privée est tout d'abord un droit constitutionnel.

L'article 20 de la Constitution, dispose que tout le monde a le droit au respect de sa vie privée et de sa vie familliale. L'intimité de la vie privée et de la vie familiale est intouchable.

L'atteinte à l'intimité de la vie privée a été incriminée dans les articles 195,196,et 197 de l'ancien code pénal.

L'article 195 dispose :

---

[167] Jacques Georges Bitoun, "De la protection de la vie privée: des cookies indigestes" www.securinet.free.fr/annexe/cookiesindigestes.html (01.09.2004).

[168] « Les Cookies Démystifiés » www.tactika.com/cookie/cookie1.htm (01.09.2004).

[169] S'il est sénateur ou ministre et qu'il visite les sites de charmes de toutes natures, il risque même d'être victime de ce qu'on appelle le "*e-blackmail*" , c'est a dire le chantage électronique.

« Crime à l'encontre de l'immunité du secret :

Si une personne ouvre intentionnellement une lettre, un télégraphe, une enveloppe fermée ne lui étant pas envoyé ou si elle saisit contrairement à l'ordre et à la procédure, le contenu d'une feuille de correspondance provenant de la poste ou du télégraphe d'un autre, sera puni de 5400 a 1800 Lires Turques d'amende,

Si l'auteur du crime en révélant le contenu de la feuille, ou allant à l'encontre de l'intimité de l'entretien par l'intermédiaire du téléphone ou télégraphe, commet un dommage sera puni d'un mois à trois ans de prison. »

L'article 196 ;

« Destruction des feuilles de correspondances :

Si une personne détruit les feuilles de correspondance provenant de la poste ou du télégraphe, sera puni, même s'il n'a pas ouvert l'enveloppe fermée jusqu'à un an de prison et de 5400 à 18000 Lires Turques d'amende.

Au cas où l'acte a causé un dommage, la peine de prison ne peut être de moins un mois et l'amende de moins de 5000 Lires Turques. »

L'article 197 ;

« Le troublement de l'intimité de correspondances :

Si une personne déclare et publie le contenu d'une lettre ou d'un télégraphe lui étant envoyé sans prendre l'autorisation de l'émetteur et cause un dommage par ce moyen sera puni de 5400 à 18000 Lires Turques d'amende. »

Dans tous les articles, les principes de publication sont énumérés : Le téléphone, le télégraphe, la poste et la lettre. İl s'agit d'une liste exhaustive.

Le principe d'interdiction de l'interprétation par comparaison en Droit pénal, empêche l'application de ces articles aux crimes commis par l'İnternet.

Le législateur turc a prévu une autre disposition dans l'article 525-a/2 de code pénal dont nous pensons qu'elle est susceptible d'être appliquée aux violations de la vie privée par l'intermédiaire de la machine informatique.[170]

Notons que l'İnfraction défini dans l'article 525-a/2 vise la protection de deux types de valeur juridique. La première est l'intérêt monétaire et économique de

[170] Yenidünya, Değirmenci, Op.cit,p.92-93

la victime. La deuxième est la vie privée, la liberté de communication, le droit au secret.

Cet article dispose que:

« Celui qui utilise, transfère ou reproduit les données, les programmes ou autres éléments enregistrés dans un système de traitement automatisé des données,dans l'intention de causer du dommage à autrui, sera punie de la même peine que celle prévue dans l'alinéa premier . »

Cet article vise à protéger les composants abstraits d'un système de traitement automatisé des données.

Ces éléments abstraits peuvent être les données (document, courrier électronique par exemple), les logiciels ou les autres éléments.

Les éléments constitutifs du crime sont :

Les actes illicites sont multiples : utiliser, reproduire ou transférer.

Il suffit d'en commettre l'un afin que le crime soit réalisé.

L'acte illicite et le résultat dommageable se reproduisent simultanément.

L'élément moral du crime est constitué d'une intention particulière : celle de causer un dommage à un tiers.

L'élément d'illégalité du crime est le manque de consentement du propriétaire du système de traitement automatisé des données.

Notons que cet article a un champ d'application restreint car,

Il recherche une intention particulière : si l'auteur du crime ne porte pas l'intention de nuire à la victime, il échappera à la peine.

D'autre part, il requiert que les éléments utilisés, reproduits, ou transférés soient enregistrés dans le système de traitement automatisé des données. Dans ce cas, le sort des programmes et des données interceptées lors de leur circulation sur le réseau reste indécis. (si un « *hacker* » par exemple, intercepte un courrier électronique entre deux individus et reproduit son contenu avant que celui-ci ne parvienne à son destinataire, il ne pourra pas être poursuivi en raison de la violation de cet article.)

Dans le nouveau Code Pénal Turc plusieurs dispositions incriminant les atteintes à la vie privée sont prévues.

La première dans l'article 132 :[171]

---

[171] Le texte en turc de l'article concerné est comme le suivant :

« Atteinte au secret de communication :

1. Celui qui porte atteinte au secret de communication entre les personnes sera puni de six mois à 2 ans de prison ou de peine pécuniaires judiciaire. Si cette atteinte au secret est réalisée par l'enregistration du contenu de la communication, la peine de prison sera d'un an jusqu'à trois ans.

2. Celui qui révèle illégalement le contenu d'une communication entre les personnes, sera puni d'un à trois ans de prison.

3. Celui qui révèle le contenu d'une communication dont il fait partie sans l'autorisation de son interlocuteur, sera puni de 6 mois à deux ans de prison ou de peine pécuniaire judiciaire.

4. Au cas où le contenu de la communication entre deux personnes est révélé par l'intermédiaire de la presse et de la publication, la peine accroira a moitié. »

Cet article ne régit que la révélation de la communication entre deux personnes. Il prévoit deux types différents de crimes : celui de tout simplement porter atteinte à la communication entre deux personnes et celui d'en révéler le contenu.

Nous pouvons dire que le premier crime prévu dans le premier paragraphe de l'article, a un champ d'application générale : le législateur a fixé l'objectif du crime et non les actes pour le réaliser. L'objectif du crime est l'atteinte au secret de communication. L'auteur du crime va pouvoir mettre en œuvre toute sorte d'actions possible pour atteindre cet objectif. S'il choisit parmi ces moyens, d'enregistrer le contenu de la communication entre deux personnes ou d'en révéler le contenu, sa peine sera accrue (la dernière phrase du premier paragraphe et le deuxième paragraphe).

"*Haberleşmenin gizliliğini ihlâl*

MADDE 132- (1) Kişiler arasındaki haberleşmenin gizliliğini ihlâl eden kimse, altı aydan iki yıla kadar hapis veya adli para cezası ile cezalandırılır. Bu gizlilik ihlâli haberleşme içeriklerinin kaydı suretiyle gerçekleşirse, bir yıldan üç yıla kadar hapis cezasına hükmolunur.

(2) Kişiler arasındaki haberleşme içeriklerini hukuka aykırı olarak ifşa eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır.

(3) Kendisiyle yapılan haberleşmelerin içeriğini diğer tarafın rızası olmaksızın alenen ifşa eden kişi, altı aydan iki yıla kadar hapis veya adli para cezası ile cezalandırılır.

(4) Kişiler arasındaki haberleşmelerin içeriğinin basın ve yayın yolu ile yayınlanması hâlinde, ceza yarı oranında artırılır." D'apres www.tcktasarisi.org (10/09/2004).

D'autre part celui qui révèle le contenu d'une communication dont il fait partie sans prendre l'autorisation de son interlocuteur, sera puni aussi.

Enfin, dans le quatrième paragraphe de l'article, une condition d'aggravation de la peine, pour tous les cas précités, est prévue : si le contenu de la communication est révélé par l'intermédiaire de la presse, les peines prévues dans les paragraphes précédents seront accrue de moitie.

Dans tous les cas une intention générale suffit à la réalisation du crime.

L'acte du crime et son résultat sont simultanés : la tentative a ce crime ne peut être possible.

Un autre article (l'article 134) incrimine la révélation des secrets de la vie privée.[172]

« Atteinte au secret de la vie privée.

1. Celui qui porte atteinte au secret de la vie privée d'une personne sera puni de 6 mois à deux ans de prison ou de peine pécuniaire judiciaire. Si cette atteinte au secret est réalisée par l'intermédiaire de l'enregistrement des images ou des voix, la limite inférieure de la peine de prison ne peut être moins d'un an.

2. Celui qui révèle des images ou des voix portant sur la vie privée d'une personne sera puni d'un an jusqu'a trois de prison. Au cas ou cet acte est réalisé par l'intermédiaire de la presse et de la publication, la peine augmentera a moitié. »

Deux différents actes, dans le but de protéger le secret de la vie privée, ont été incriminés dans cet article.

Dans le premier paragraphe de l'article un crime général d'atteinte au secret de la vie privée est prévue. Le législateur a évité d'énumérer les moyens pouvant être mis en œuvre pour le réaliser : toutes sortes d'actions susceptibles de

---

[172] Le texte en turc de l'article concerné est comme le suivant

"*Özel hayatın gizliliğini ihlâl*

MADDE 134- (1) Kişilerin özel hayatının gizliliğini ihlâl eden kimse, altı aydan iki yıla kadar hapis veya adli para cezası ile cezalandırılır. Gizliliğin görüntü veya seslerin kayda alınması suretiyle ihlâl edilmesi hâlinde, cezanın alt sınırı bir yıldan az olamaz.

(2) Kişilerin özel hayatına ilişkin görüntü veya sesleri ifşa eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. Fiilin basın ve yayın yoluyla işlenmesi hâlinde, ceza yarı oranında artırılır." D'apres www.tcktasarisi.org (10.09.2004).

porter atteinte au secret de la vie privée seront punis. Quelques une d'entre elles seront même punies plus gravement : si l'atteinte au secret de la vie privée est réalisé par l'enregistrement des images et des voix, la limite inférieure de la peine de prison ne peut être moins d'un an. (La limite supérieure étant de deux ans)

Au cas où ces images ou voix enregistrés sont révélés à autrui, la peine sera d'avantage plus lourde : la peine de prison pourra être évalué d'un an à deux. Une condition d'aggravation de la peine est prévue aussi : si la révélation d'image et de voix est faite par l'intermédiaire de la presse, la peine sera accrue a moitié.

Dans tous les cas une intention générale est suffisante.

La tentative incomplète et la tentative complète sont possibles.

Le Nouveau Code Pénal prévoit aussi deux autres articles sur l'enregistrement des données personnelles : les articles 135 ;

« Enregistrement des données personnelles :

1. Celui qui enregistre illégalement les données personnelles sera punis de 6 mois à trois ans de prisons.

2. Celui qui enregistre illégalement les données personnelles relatives à l'opinion politique, philosophique ou religieux, aux origines raciales, aux penchants moraux, à la vie sexuelle, à l'état de santé ou aux liens syndicaux d'une personne sera punis de la même manière que dans le paragraphe précédent. »

Cet article régit la saisine illégale des données personnelles.

Là, contrairement aux articles précédents l'acte permettant la réalisation du crime est décrit dans le texte de l'article. : Il s'agit du fait d'enregistrer.

L'acte et son résultat sont simultanés : le crime sera réalisé des lors que l'acte sera accompli.

Une intention générale est requise : celle d'enregistrer les données personnelles suffit.

D'autre part, il faut que cet enregistrement soit illégale (élément d'illégalité). Au cas où l'enregistrement se fait conformément à la Loi, il est évident que le crime ne se réalisera pas.

Cependant une forme spéciale du crime est prévu dans le paragraphe suivant sans pour autant aggraver la peine: si l'enregistrement est faite en vue

d'obtenir les données relatives portant à l'opinion politique, philosophique ou religieux, aux origines raciales, aux penchants moraux, à la vie sexuelle, à l'état de santé ou aux liens syndicaux d'une personne, la peine sera la même que celle dans le paragraphe précédent, c'est-à-dire, de six mois a trois ans de peines de prison.

Et l'article 136 ;

« Celui qui donne à autrui, divulgue ou obtient illégalement les données personnelles d'une personne sera puni d'un an à quatre ans de prison. »

Une forme spéciale du crime prévu dans l'article précédent est régie ici.

L'article précédent prévoyait l'enregistrement illégal des données personnelles appartenant à autrui. Celui-ci prévoit la divulgation des données enregistrées. L'acte est plus sévèrement puni dans ces conditions : la peine est d'un à quatre ans de prisons.

Les actes menant à la réalisation du crime sont énumérés dans le texte de l'article : ce sont les faits d'obtenir, de donner à autrui et de divulguer les données personnelles d'une personne. Ces actes doivent être réalisés d'une manière illégale : C'est-à-dire l'agissement ne doit pas être conforme a la Loi.

Une intention générale est suffisante.

La tentative est possible.

La Loi sur le Nouveau Code Pénal Turc prévoit donc un arsenal répressif complet au sujet des atteintes à la vie privée.

Ainsi toute sorte d'obtention d'information relative à la vie privée d'une personne va pouvoir être incriminée et punie.

La plupart du temps le législateur n'a pas énuméré les supports de publications : il a évité de faire une liste exhaustive afin de pouvoir prendre en compte tous les développements technologiques, y compris l'İnternet.

3. Les Infractions de presse sur Internet

a. Les différentes infractions de presse pouvant être commises sur Internet.

Ces infractions sont nombreuses et leurs finalités sont totalement différentes. Leur seul point commun est l'exigence de publicité. La publicité implique que le message ne soit pas adressé à une seule personne déterminée mais diffusé à l'intention du public, de l'inconnu et d'auditeurs éventuels et potentiels.[173]

Ces infractions peuvent être classées de la manière suivante :

Certaines provocations sont incriminées en tant qu'infraction obstacle c'est-à-dire indépendamment des résultats qui auront pu en résulter : Il s'agit d'éviter que cette provocation ne soit suivie d'effet réel.

Cette catégorie regroupe la provocation au suicide, la provocation au meurtre, la provocation à l'atteinte volontaire de l'intégrité de la personne, à l'agression sexuelle, à la haine raciale ou à la violence (qui est la provocation a l'égard d'une personne ou d'un groupe de personnes à raison de leur origine, de leur appartenance ou de leur non appartenance à une ethnie, une nation, une race ou une religion peu importe le mobile, dés lors que la provocation revêt un caractère direct). L'apologie des crimes contre l'humanité en particulier des crimes de génocide et les actes de terrorismes.

Une autre catégorie de crime est formée par les délits d'opinion motivés par la protection d'ordre public. Ces infractions sont directement plus liées à l'audience que peut avoir le message et risquent d'être moins souvent poursuivis sur le réseau. Sont principalement visées l'atteinte à l'autorité d'un chef d'Etat, la divulgation d'élément d'un dossier en instruction et l'atteinte à l'indépendance et de la dignité de la justice.

Enfin, la dernière catégorie est celle des infractions de presse visant les personnes. Il s'agit de manière générale d'éviter toute atteinte à la personnalité du mineur (en notre matière, il s'agira principalement de l'envoi de courriers électronique ou de fichiers susceptible d'heurter la morale du mineur.), de lutter contre la diffamation, l'injure, et dénonciation calomnieuses qui sont des infractions très répandues sur Internet, et de lutter contre les atteintes à la mémoire des morts.

---

[173] Pansier – Jez, Op.cit, p.79.

b. La Répression

Le Législateur turc a décidé que les crimes de presse commis sur İnternet soient traités de la même manière que les crimes de presse ordinaire, a fait pénétrer ces crimes dans le champ d'application du code de la Presse, avec l'article 26 de La Loi no 4756 prévoyant des amendements dans la Loi concernant le Conseil Supérieur de la Radio-Télévision, dans le Code de la Presse, dans la Loi concernant les İmpôts sur le Revenu.[174]

Le texte de l'article 26 est comme le suivant :[175]

« Art.26 : L'article supplémentaire suivant a été ajouté à la Loi no 5680 :

Les dispositions de cette Loi portant sur les préjudices matérielles et morales provenant de la nouvelle mensongère, sur l'insulte et d'actes semblables seront appliquées à toutes sortes d'écriture, de dessin, de signe, d'image sonore ou insonore et ses semblables publiés sur les technologies informatiques, à l'ouverture d'une page sur İnternet ou sur un journal électronique ou sur un bulletin électronique ou ses semblables etc. »

Les délits cités dans le paragraphe précédent, n'ont évidemment pas été prévus pour s'appliquer sur İnternet.

Mais ces infractions concerne le contenu et non le support.

Il n'y a donc aucune raison de ne pas étendre leur champ d'application, à la mise à la disposition du public par voie électronique.

Toutefois de même qu'il a fallu aménager, certaines modalités procédurales pour la prise en compte de la radiodiffusion quelques points de conflits peuvent surgir entre la structure d'İnternet et la conception de la répression.

---

[174] Le nom de la Loi en turc est :
"RADYO VE TELEVİZYONLARIN KURULUŞ VE YAYINLARI HAKKINDA KANUN, BASIN KANUNU, GELİR VERGİSİ KANUNU İLE KURUMLAR VERGİSİ KANUNUNDA DEĞİŞİKLİK YAPILMASINA DAİR KANUN"

[175] Le texte en turc de l'article concerné est comme le suivant:
" ***MADDE 26.*** *– 5680 sayılı Kanuna aşağıdaki ek madde eklenmiştir.*

EK MADDE 9. – Bu Kanunun yalan haber, hakaret ve benzeri fiillerden doğacak maddî ve manevî zararlarla ilgili hükümleri, bilişim teknolojileri ve internet ortamında sayfa açılması veya elektronik gazete, elektronik bülten vb. suretiyle yayınlanan her türlü yazı, resim, işaret, sesli veya sessiz görüntü ve benzerleri hakkında da uygulanır." D'apres www.hukuki.net/mevzuat (26/04/2004).

« La soumission d'İnternet au Droit de la presse ne saurait pas être une simple transposition des règles appliquées à la presse écrite ou même aux moyens de communication audiovisuelle. »[176]

Or ces conflits potentiels n'ont pas été pris en compte par le Législateur Turc.

Les raisons des problèmes pouvant surgir sont les suivants :

D'abord tout sur İnternet ne correspond pas à une communication au public ou alors dans une mesure différente.

Le Web est certainement le service sur İnternet qui se rapproche le plus d'un service éditoriale classique, mais il ne faut pas oublier néanmoins les forums, l' « *İrc* », les « *NewsGroup* », les « *E-mail* » adressées à des listes de diffusion.

D'autre part, le Code de la Presse a prévu pour les crimes de presse certaines spécificités.

Un délit pour être considéré comme délit de presse doit porter les caractéristiques suivantes :

Premièrement, le sujet du délit de presse doit être une œuvre imprimée qui doit soutenir des idées, doit avoir une existence matérielle et afin d'être publié doit être imprimé à l'aide des outils de presse ou reproduit par des outils semblables.

Deuxièmement, l'œuvre imprimée doit être publiée

Les différents modes de publications sont selon l'article 3/2 du Code de la Presse les suivants ; la distribution, la vente, la projection, la suspension, la mise à l'écoute et la commercialisation.

Les délits commis sur İnternet afin d'être considérés comme délits de presse, doivent porter les caractéristiques suscités or cela ne semble pas être possible.

Bien que les publications sur İnternet contiennent des idées ; elles ne disposent pas d'une existence matérielle. La mise à la disposition de l'internaute d'une page Web ne saurait être en aucun cas une impression à l'aide des outils d'imprimerie ou de presse.

D'autre part ; dans la presse classique, ce qui est important c'est l'exemplaire à produire. Cet exemplaire sera reproduit qu'une seule fois, sera par la suite transféré à l'imprimerie. L'exemplaire dans la presse écrite ne change jamais, il

---

[176] Auvret P, "L'application du Droit de la Presse au réseau İnternet"
JCP no 5 3 février 1999 p. 257.
D'après Jougleux,op.cit, p.93.

est définitif. Or une publication İnternet peut être changée par le fournisseur du contenu, plusieurs fois dans une même journée.

Donc, l'interprétation des publications sur İnternet comme des publications de presse, aboutira à la négation des spécificités de la presse électronique et sera ainsi fautive.[177]

Des problèmes se posent aussi au sujet du droit de réponse et du délai de prescription.

Premièrement le droit de réponse est prévu dans l'article 32 de la Constitution : « le droit à la correction et le droit de réponse sont reconnus aux individus quand leur dignité et leur honneur sont touchés ou quand des publications leur concernant et allant a l'encontre de la vérité sont réalisés.

Si la correction et la réponse ne sont pas publiés, le juge décide dans sept jours à partir de la demande sur la nécessité de publication.

Le droit de réponse est conçu comme s'inscrivant dans le fil d'un débat chronologique, alors qu'İnternet ouvre la voie au débat simultané.

De plus il n'est pas toujours possible d'assurer au droit de réponse une audience similaire à celle du message incriminé.

Le délai de réaction est de deux mois, ce qui peut sembler un peu court pour le réseau İnternet dans lequel l'information noyée sous une masse de donnée devient parfois plus inaccessible que par des moyens classiques.

Quand au délai de prescription ; les actions en délit de presse se prescrivent par deux mois à compter de la première publication. Si le point de départ de ce délai est aisément cernable lorsque le délai est commis dans le cadre de la diffusion d'un écrit ou d'une émission radiophonique ou télévisuelle, la question devient plus complexe dans le cadre d'une diffusion en ligne. En effet, les infractions de presse constituent des infractions instantanées car son élément matériel c'est-à-dire la publication de l'information litigieuse est elle-même instantanée, alors que les éléments contenus sur un site Web sont maintenus en ligne sur une longue durée. C'est la raison pour laquelle il est difficile de transposer la notion de publication en

---

[177] İlkiz, Fikret "3984 sayılı Radyo ve Televizyon ların kuruluş ve yayınları hakkında Yasa Tasarısı ve Basın Yasası değişiklikleri ile İnternet yayıncılığı düzenlemesinin yarattacağı sorunlar." S.22 vd. d'après Sınar ,op.cit, p.140

matière de diffusion sur Internet. Ainsi le délai de prescription semble inadapté à la réalité des choses voire injuste. La difficulté la plus importante consiste dans la recherche de la date de la première publication du message destiné à un forum, du mail diffusé à un nombre indéterminé de personne, du téléchargement du site Web sur le serveur. Non seulement, cette date dans l'absolue est aisément manipulable mais encore elle se révèle impossible à déterminer.

Nous pouvons donner ici comme exemple la décision de la cour d'appel de Paris du 15 décembre 1999 portant sur l' « affaire Jean Louis C. »

Ce dernier, artiste autoproclamé, avait mis en ligne sur son site Web, quelques textes de chansons violemment racistes. Le TGI de Paris avait fondé une décision de relaxe sur la prescription de l'action publique.

La cour d'appel a reformé cette décision. Son raisonnement a été le suivant : si la date de la première mise à disposition du public, le point de départ des infraction de presse, correspond à un acte précis en matière audiovisuelle et résulte du support en matière d'écrits, il n'en va pas de même lorsque le message a été publié sur Internet qui constitue un mode de communication dont les caractéristiques techniques obligent à adapter les principes posés par la Loi sur la Presse. Sur le réseau, le trouble causé à l'ordre public ou le préjudice causé à des tiers ne s'éteint pas du fait de l'écoulement du temps. Surtout, la publication résulte de la volonté renouvelée de l'émetteur qui place le message sur son site, choisit de l'y maintenir ou de l'en retirer quand bon lui semble. L'acte de publication devient ainsi continu.

En d'autres termes, tant que l'émetteur maintient le message, sa volonté délictueuse est réitérée. En conséquence, le délai de prescription est gelé tant que le texte litigieux est maintenu sur le site.

Il était donc plus évident d'élaborer une Loi portant sur les diffusions en lignes plutôt que de les prendre en compte dans le cadre du code de la presse.

Sous section III : Autres Types de délits : la Falsification İnformatique

La falsification informatique est souvent accompagnée du délit de fraude informatique. Mais le fait que ces crimes sont destinés à protéger deux valeurs différentes (la fraude : l'ordre public ; la falsification : la confiance publique), nous conduit à les traiter séparément.

La falsification informatique est à présent régie par l'article 525 / c du code pénal.[178] :

« Celui qui dans l'intention d'utiliser comme preuve dans le domaine de la justice, installe dans le système de traitement automatisé des données des informations ou d'autres éléments ou change les informations et les autres éléments existants dans le système pour former un document faux, sera punis d'un an a trois de prison, celui qui utilise le document formé tout en sachant qu'il est faux, sera puni de six mois à deux ans de prison. »

L'article 525/c du code pénal Turc, bien qu'il ne soit formé d'un seul paragraphe ; contient deux crimes différents :

- celui de former un document faux par l'intermédiaire des données contenues dans le système de traitement automatisé des données (soit en plaçant des nouvelles données, soit en changeant les existants.)
- celui d'utiliser le document ainsi formé.

Ce crime est une forme spéciale du délit de faux. Ce dernier ne pouvant pas être appliqué aux crimes semblables commis par l'intermédiaire d'un ordinateur, en raison de l'interdiction de l'appréciation comparative en Droit pénal, le législateur turc a ressenti le besoin de créer un nouveau type de crime afin de pouvoir poursuivre ces infractions.

Dans cet article une nouvelle définition du « document faux » est donné :

Le législateur a créé un nouveau type de document juridique pour instaurer dans les relations juridiques, une confiance aux preuves formées à l'aide de l'ordinateur.

---

[178] Le texte en turc de l'article concerné est comme le suivant:
"*TCK mad.525/c : Hukuk alanında delil olarak kullanılmak maksadıyla sahte bir belgeyi oluşturmak için bilgileri otomatik işleme tâbi tutan bir sisteme, verileri veya diğer unsurları yerleştiren veya var olan verileri diğer unsurları tahrif eden kimseye bir yıldan üç yıla kadar, tahrif edilmiş olanları bilerek kullananlara altı aydan iki yıla kadar hapis cezası verilir.*"

Avec cette nouvelle définition de « document », les informations stockées à l'intérieur de l'ordinateur y gagne une valeur juridique.

Surtout les informations stockées portant sur le registres des casiers judiciaires, des statistiques relatives aux événements, des informations relatives au criminels et ceux qui ont été pris en garde à vue y sont visées.

Le changement de ce genre d'informations en pénétrant dans le système de traitement automatisé des données constitue ainsi le délit de faux informatique.

Par exemple, bien qu'il n'ait rien obtenu au concours de placement aux universités, celui qui pénètre dans l'ordinateur central et se rajoute parmi ceux qui ont réussi au concours, aura ainsi commis le délit de faux informatique.

Le deuxième délit prévu dans l'article, est celui de l'utilisation du document faux ainsi formé.

Ces deux crimes sont indépendant l'un de l'autre. Le premier se rapporte à la création d'un document faux, alors que le deuxième concerne son utilisation.

Tout de même, il faut que la première infraction soit commise par une personne, afin que la deuxième puisse être réalisée. La première infraction est la condition préliminaire de la deuxième.

Le législateur a expressément prévu pour la deuxième infraction, l'auteur du crime doit savoir que le document utilisé est faux. Cela est valable surtout pour le cas ou celui qui l'a créé et celui qui l'utilise sont des personnes différentes.

La valeur juridique protégée dans cet article est la même que celle protégée par le délit de faux ordinaire : le législateur veut protéger la confiance du public aux documents utilisés dans les relations juridiques.

Les éléments matériels du crime sont :

Le sujet du crime est l'ensemble des données contenues dans un ordinateur et ayant la qualité de preuve en justice.

Le sujet du deuxième crime est le document obtenu à l'aide des manipulations faites ainsi. Ce document peut être matérielle ou bien virtuelle.

L'acte du premier crime est à choix multiple : installer des données ou changer des données.

L'acte du deuxième crime est l'utilisation du document dont il sait sa qualité de faux, de manière à produire des résultats dans le champ juridique.

L'acte et le résultat des deux crimes sont simultanés : le résultat de l'acte est réalisé dés lors que l'acte est commis.

La tentative incomplète à ce crime peut être envisagée.

L'élément morale de la première infraction est une intention particulière : l'auteur du crime doit agir avec l'intention d'utiliser le document formé comme preuve dans le domaine juridique.

L'élément moral du deuxième crime est générale.

La peine prévue est plus lourde dans le premier cas : elle va d'un à trois ans de prison. Pour l'utilisation du document faux, la peine prévue varie entre 6 mois et deux ans de peine de prison.

Sur la Loi sur le nouveau Code Pénal Turc cette disposition ne figure pas. Le législateur a préféré définir plus largement le délit de falsification, de manière à englober les documents formés à l'aide d'un système informatique.

Dans le cadre des délits informatique, à l'article 245/2[179] du nouveau Code pénal, le législateur a préféré traiter une forme plus spéciale de délit de falsification, celui relatif aux cartes de crédit.

« Celui qui procure un bénéfice pour son propre compte ou pour celui d'autrui en créant ou en utilisant une banque ou une carte de crédit falsifiée sera puni, au cas ou son acte ne constitue pas un autre crime dont la peine est plus lourde, de quatre a sept ans de prison. »

İci, le but de la criminalisation de cet acte est la protection de la confiance du public aux institutions financières tels que les banques et les moyens de paiement comme les cartes de crédit.

Les actes permettant la réalisation du crime sont soit la formation d'une fausse banque ou d'une fausse carte de crédit, soit leur utilisation.

---

[179]Le texte en turc de l'article concerné est comme le suivant :

MADDE 245- (1) Başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırtarak kendisine veya başkasına yarar sağlarsa, üç yıldan altı yıla kadar hapis cezası ve adli para cezası ile cezalandırılır.

(2) Sahte oluşturulan veya üzerinde sahtecilikyapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlayan kişi, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, dört yıldan yedi yıla kadar hapis cezası ile cezalandırılır.

D'après www.tcktasarisi.org (10.09.2004).

Le résultat de ces actes est la procuration d'un bénéfice pour son propre compte ou celui d'autrui.

Une intention particulière est requis : non seulement, l'auteur du crime doit savoir et vouloir le résultat de son acte, mais il doit aussi avoir l'intention de procurer un bénéfice pour son propre compte ou pour celui d'autrui.

L'élément d'illégalité est la fausseté de la banque ou de la carte de crédit crée. Si ces deux sont formés en présence d'une prérogative attribuée par la loi, l'acte ne saurait être incriminé.

La tentative complète et la tentative incomplète sont possibles.

Troisième Partie : La Régulation des Infractions sur Internet

La régulation des infractions sur Internet peut s'effectuer à trois niveaux. Au niveau de l'Internet même : les internautes et les professionnels de l'Internet ont élaboré un certain nombre de règles éthiques auxquelles tous les utilisateurs de l'Internet sont tenus d'obéir. Or ce procédé d'autorégulation est loin d'être dissuasif et ne parvient pas à empêcher les esprits malsains d'accomplir leurs actes criminels. Dés lors, l'intervention de l'Etat est nécessaire. Cependant cela doit s'opérer d'une manière vigilante, afin de ne pas transgresser les droits et les libertés fondamentales sur Internet. D'autre part, l'intervention des Etats aux crimes commis sur Internet et ayant des conséquences sur leur territoire ne semble pas être, non plus, à elle seule suffisante. En effet, tous les systèmes législatifs sont hétérogènes et les conflits de valeur morale posent l'essentiel du problème : tous ces systèmes législatifs n'incriminent pas les mêmes faits et répriment les mêmes actes de manière différente. Ainsi un propos incitant à la haine raciale proposée sur un serveur américain n'enfreint en aucun cas à la loi dudit pays tandis que le même propos est sévèrement combattu dans les pays de l'Europe Occidentale. L'affaiblissement des principes du droit pénal par ces conflits de loi interne et externe a poussé les pays européens à coopérer dans la lutte contre la criminalité sur Internet et à déterminer un droit unique qui s'y substituerait à la multiplicité des lois applicables sur Internet. Ainsi nous traiterons dans une troisième sous partie la Convention Européenne sur la Cybercriminalité.

Chapitre I : L'Autorégulation

L'autorégulation pourrait s'appeler en réalité la régulation par la voie privée. Elle dépend d'individus ou d'entreprises qui fixent les règles de base sous une forme contractuelle ou en s'autolimitant sur une base volontaire et concertée.

Nous examinerons sous cette appellation les règles formant l'éthique de l'Internet ou la Netiquette, les moyens de lutte individuels tels que le cryptage et le filtrage, ainsi que les moyens de corégulation.

Section I : La Netiquette

Sous section I : Le contenu de la Netiquette

La Netiquette est l'œuvre d'étudiants ou d'universitaires dans le temps ou l'Internet servait principalement d'outil informationnel.

La Netiquette est la charte de bonne conduite des acteurs de l'Internet qu'ils soient utilisateurs professionnels ou particuliers.

Elle est comparée à un ensemble de règles de civilité et de protocole. Elle comprend toutes les règles de comportements acceptables par les usagers de l'Internet. L'idée est d'organiser une sorte de discussion entre « gentlemen » et les services de discussions par forum y sont principalement visées.

La Netiquette cherche à lutter contre plusieurs types de cybercriminalité lié à une activité plus ou moins éditoriale.

Elle édicte un certain nombre de principes nécessaires pour savoir communiquer sur Internet. La présentation de ces principes est assez ludique puisce qu'elle prend la forme de commandements[180] :

« - Administrateur, tu n'agresseras pas,
- La prudence dans les écrits tu emploieras,
- Brièvement tu écriras,
- Des titres clairs tu choisiras,
- A l'audience toujours tu penseras,
- A l'humour et au sarcasme tu prendras garde,
- Une seule fois ton message tu posteras,
- Par Mail, le plus souvent tu répondras,
- Un résumé tu posteras,
- L'entête tu vérifieras,
- Les droits des auteurs tu respecteras,
- Les références tu citeras,
- Les remontrances orthographiques tu éviteras,
- La signature, tu n'exagéreras pas,
- La longueur des lignes tu limiteras,

[180] www.cyberworkers.com/ledroit.fr/index-nétiquette.shtml (09.12.2003.

- Les caractères de contrôle tu éviteras,
- A tes annonces publicitaires, tu résisteras. »

Sous section II : L'Intêret juridique de la Netiquette.

Plusieurs types de contrats sont susceptibles de rendre compte de la Netiquette, en vue de l'insérer dans la liste des obligations d'une ou des deux parties.

La Netiquette acquiert alors force juridique au même titre qu'un renvoi dans le contrat vers une clause spéciale.

Les contrats portant la mention de la Netiquette sont souvent des contrats d'adhésion. C'est notamment le cas de contrats de fourniture d'accès à Internet et dans lequel figure une clause relative à Internet de façon explicite ou implicite.

Le non-respect de la Netiquette par l'utilisateur peut entraîner la suspension et la coupure de son compte.

Les premières décisions en Droit comparé, notamment en France, a reconnaître la légitimité d'une coupure de compte sur la base de la Netiquette ont été rendues par le Tribunal de Grande Instance de Rochefort sur Mer en 2001, et celui de Paris en 2002.[181]

En ce qui concerne l'arrêt rendu par le tribunal de Rochefort sur Mer, en l'espèce, le défendeur dans le cadre de son abonnement « *Wanadoo* », a déposé de nombreux messages publicitaires sur différents forums de discussions en vue de développer ses activités. Le « *Spamming* » a été si intense qu'il a amené de très nombreux utilisateurs à le dénoncer au fournisseur d'accès. Ce dernier a interrompu son service après l'avoir mis vainement trois fois en mis en garde. Le Tribunal a donné raison au demandeur (La société anonyme France Télécom Interactive.) et a condamné le défendeur à une allocution de 914.69 Euros.

Nous pouvons encore citer l'exemple de la première décision canadienne traitant d'une affaire relative aux courriers non sollicités et de la mise en œuvre des règles de la Netiquette[182].

En l'espèce le prestataire de Service à l'Internet de Toronto (« *Nexx Online* ») décide de fermer le compte d'hébergement d'un de ses clients « *Ontario Inc.* », gestionnaire de « *beaverhome.com* ». Le motif invoqué est le suivant : depuis

---

[181] www.forumetinternet.org/documents/jurisprudence/lire.phtml?id.260 (17/12/2003).

[182] www.cyberworkers.com/ledroit.fr/index_netiquette.shtml (17/12/2003).

le mois de mars 1999 « *beaverhome.com* » avait procédé a l'envoi journalier de plus de 200 000 messages non sollicités via les services d'un tiers prestataire.

L'intérêt du présent jugement réside essentiellement dans l'argumentation du juge qui mène à conférer la force juridique aux règles de la Netiquette par le biais contractuel.

Enfin le juge n'a pas hésité à déclarer que la société défenderesse a agi en violation des termes du contrat incluant le respect aux principes de la Netiquette. Ainsi la pratique du « *spamming* » au mépris de la déontologie du réseau a justifié la déconnexion du site « *beaverhome.com* »

Il faut noter que, les règles de la Netiquette sont insuffisante pour assurer la régulation de l'Internet. De plus, dans tous les cas, la dimension partiellement contractuelle de la Netiquette ne peut aboutir qu'à des conséquences civiles. Par contre la reprise des dispositions de la Netiquette dans un procès pénal ne peut sembler possible.

Section II : Les moyens de Lutte individuels contre la cybercriminalité

Sous section I : L'encryptage

L'encryptage est un concept très ancien puisce qu'il a été utilisé par les plus antiques civilisation.

Le premier véritable encryptage (à savoir la transformation d'un texte clair en texte codé) a eu lieu sous le règne de Jules César.[183]

Cependant et malgré l'âge très respectable de ces techniques, l'encryptage n'a connu son essor et sa pleine efficacité qu'avec l'utilisation de l'informatique.

Il a fallu garantir la sécurité des informations, les transactions faites via Internet pouvant être facilement intercepté. Cela s'est fait à l'aide de l'encryptage.

La cryptologie est l'art de rendre les données secrètes. Elle permet ainsi de protéger un message des regards indiscrets. Elle est essentiellement basée sur l'arithmétique. Il s'agit de transformer les lettres qui composent le message en une succession de chiffres sous formes de bits (car l'informatique est basé sur le système

[183] "Introduction a l'encryptage" d'après http://membres.licos.fr/nanaud/encryptage/introduction/intro.htm?(06.08.2004).

binaire) puis ensuite de faire des calculs sur ces chiffres pour d'une part les modifier et de faire en sorte que le destinataire sache le décrypter. [184]

Le fait de coder un message de telle façon à le rendre secret s'appelle cryptage (ou chiffrement). La méthode inverse consistant à retrouver le message original, est appelé décryptage.

Les partisans de l'autorégulation de l'Internet se sont très vite emparés du problème et en ont fait leur cheval de bataille. La notion d'autorégulation est montrée comme indissociable de la cryptologie. Mais la démonstration est faite qu'avec peu de volonté[185].

Les Etats se montrent en général réticents au sujet de la libéralisation de la cryptologie.

Aux Etats Unis par exemple ; C'est le département de la défense nationale qui se montre contre cette libéralisation. Notamment le Bureau Fédéral de l'İnvestigation (FBİ) et le Service National de l'İntelligence Criminelle (NCİS) craignent que cette technologie soit utilisée par des criminels afin de dissimuler les preuves de leurs délits. Cela risque d'entraîner des résultats graves et irréparables notamment dans le cadre du terrorisme, du trafic de drogue et de la criminalité organisée. Dans certains événements terroristes, des plans d'attaque cryptés ont été obtenus par la police.

De même en Angleterre, « l'affaire Starbust »[186] fournit un bon exemple aux méfaits du cryptage :

L'affaire Starbust est une opération accomplie au niveau international comprenant les Etats-Unis, l'Angleterre, l'Afrique du Sud et les pays de l'Asie du Sud Est, et ayant servi à l'arrestation de 37 personnes adhérentes à une organisation pédophile : leur chef était un prêtre à l'église de Saint Joseph à Durham Gilsgate en Angleterre. Ce prêtre, Adrien McLeish disposait de la plus grande collection de photographes de pornographie enfantine jamais saisie par la police jusqu'à ce jour. McLeish commercialisait ces photos depuis des années par l'intermédiaire des courriers électroniques cryptés. Le cryptage était la raison pour laquelle la police n'avait pas réussit à l'attraper pendant des années. Pour finir, McLeish fût jugé par la

---

[184] « La cryptologie » http://securinet.free.fr/cryptologie.html (06.09.2004).

[185] « Cryptologie, moyen de sécuriser, les échanges » http://jurisexpert.net /site/fiche.cfm ?id_fiche=1213 (15.09.2004) .

[186] Sınar, op.cit,p.60.

cour correctionnelle royale de New Castle Upon Tyne et fût condamné le 13 Novembre 1996 à 6 ans de prison.[187]

En France, la cryptologie a longtemps été l'objet d'un monopole de l'Etat du fait du régime très strict de sa mise en œuvre. La libéralisation du cryptage la plus significative au cours du temps fût le décret du 19 janvier 1999 selon lequel le seuil de cryptage fut élevé à 128 bits ce qui devrait assurer la sécurité des transactions sur İnternet. Ce décret est important aussi parce qu'il dispense de formalité les autres opérations sur ces logiciels ou matériels. (Sont permises ainsi, sauf quelques exceptions, l'utilisation, l'importation et l'exportation des logiciels de cryptage.)

Avec la libéralisation de logiciels de cryptage il est possible d'affirmer qu'un certain type de cybercriminalité disparaîtra en France. Mais il faut aussi soutenir que la cybercriminalité a gagné une arme de poids. İl est dans tout les cas très difficile car complexe d'atteindre un équilibre dans la balance des intérêts en jeu dans ce domaine. On ne peut prédire à l'heure actuelle si la cryptologie servira ou desservira la cybercriminalité malgré les affirmations péremptoires des professionnels de l'İnternet favorable au retrait de l'Etat de l'İnternet.

En Turquie ; l'utilisation de la cryptologie est interdite dans la communication faite par l'intermédiaire des appareils sans fil. Cette interdiction est instaurée par l'article 30 de la Loi portant sur les appareils de communication sans fil no : 2813 promulguée le 05.04.1983 et publié dans le journal officiel du 07.04.1983 no 18011.

Selon cet article, la communication cryptée au moyen des appareils sans fil est interdite pour les personnes morales privées et les personnes physiques. Les organisations publiques disposant de la prérogative d'utiliser la cryptologie sont les forces armées turques, le commandement de la sécurité maritime, l'organisation nationale de l'information, la direction générale de la sécurité nationale et le ministère des affaires internationales.

Ceux qui agissent contrairement à cet article risque d'être puni de six mois à un an de prison en temps normal, de un à deux de prison en temps d'état de siège et de mobilisation.

İl est à noter que cette loi ne concerne que les communications établies par l'intermédiaire des appareils sans fils tels que la radio, les télégraphes ou les

---

[187] Smar, Op.cit, p.60.

« Walkie-talkie ». Elle a été promulguée à une époque ou l'expansion de l'İnternet ne pouvait être imaginée. Du coup tant que la connexion İnternet n'est pas établie à l'aide des ondes radiographiques, ce qui est évidemment très rare, cette loi ne s'appliquera pas. Nous pouvons ainsi dire que la communication cryptée via İnternet est relativement libre en Turquie.

Sous section II : Le filtrage

En Europe, l'idée selon laquelle un contrôle de l'İnternet pourra être organisé par le biais d'institutions privées perdure.

Le fonctionnement de ce type de contrôle est comparable à celui d'un annuaire en ligne : un personnel par l'intermédiaire d'une enregistrement en ligne seraient chargés de repérer les sites posant quelques difficultés et de leur attribuer une numérotation. Les sites pourraient être placé selon leur contenu sexuel ou leur opinion politique déviante. Un logiciel installé sur l'ordinateur de l'utilisateur refuseraient l'accès à ces sites a la personne ne possédant pas l'accréditation suffisante et une mise à jour en ligne et automatique de sa base de données peut être envisagé simplement.

Un tel système est condamné à l'échec car il ne prend pas en compte la flexibilité du réseau, les sites pouvant instantanément « voyager » d'une adresse à une autre ou même cohabiter sur différents endroits du net (les sites miroirs.).

Section III : La corégulation

La tendance actuelle, dans plusieurs pays européens est la promotion d'une logique de corégulation.

L'idée de corégulation est en fait un rapport entre les pouvoirs publics et les acteurs de l'İnternet. Sous cette idée, la régulation de l'İnternet est la responsabilité partagée par la société et par conséquent comprend les acteurs de la voie publique. L'idée consiste à adjoindre à la puissance publique des acteurs privés et des mécanismes librement consentis. La corégulation est le transfert des responsabilités traditionnellement publiques vers des acteurs indépendants qui assurent une mission de régulation.

Nous allons d'abord examiner le droit comparé avant d'aborder la situation en Turquie.

Sous section I : Le Droit comparé

En France, ce sont le CSA, l'ART et le CNİL qui assurent cette fonction.

Leur mission essentielle n'est pas de décider du choix d'un système ou d'un technologie mais de faire en sorte que ce choix respecte un certain nombre de règles afin d'éviter qu'il n'aboutisse à de effets pervers ou à des conséquences dangereuses.

La CNİL (Comission Nationale des İnformatiques et des Libertés) tout d'abord intervient pour veiller à l'application de la Loi de 1978, donc pour tout ce qui touche aux données nominatives et à leur traitement automatisé et, İnternet en comporte beaucoup. İl s'agit de la première expérience d'autorité administrative indépendante, ce qui montre à quel point les nouvelles technologies ont joué le rôle de cheval de Troie de la philosophie visant à l'autorégulation en France.[188]

L'ART (Autorité de Régulation des Télécommunications) créée par la Loi du 26 Juillet 1996 est aussi compétente pour l'İnternet.[189]

Le CSA (Conseil Supérieur de l'Audiovisuel) après avoir longtemps ignorée les nouvelles technologies a opéré un revirement politique et s'intéresse désormais à l'Internet. Sa position est claire : « la position d'İnternet ne pose aucun problème dés lors l'on comprend que les différents services proposés sur İnternet ne sont pas structurellement différents des mêmes services proposés par des moyens plus traditionnels ».[190]

Cependant l'indépendance du CSA et du CNİL est douteuse car leurs membres sont élus par le corps politique.

En Angleterre, le comité de l'observation de l'İnternet fondé en 1996 (İnternet Watch Foundation) assure cette fonction.

---

[188] Jougleux, Op.Cit, p.202.
[189] İbid., p.202.
[190] Vitalis A. "le contrôle politique des technologies" Edition l'Harmattan,1992 p.203. d'apres Jougleux,op.cit, p.203.

L'augmentation des publications illégales sur İnternet en Angleterre a provoqué des tensions dans le public. En conséquence, l'association des fournisseurs d'accès à İnternet anglais « İSPA-UK » a entrepris une série de négociation avec le gouvernement qui a aboutit à la création d'un organisme hybride formé des fournisseurs d'accès à İnternet et des représentants d'organisations civiles.

L'İWF a réalisé de grands travaux sur les publications illégaux sur İnternet, notamment sur la prévention de la pornographie enfantine.

Sous section II : le Droit turc et le conseil de l'İnternet.

Le Conseil de l'İnternet est un organisme fondé au sein du ministère de la communication.

Ses principales fonctions sont :

- La détermination des buts à court et à long terme concernant l'infrastructure de l'İnternet.[191]

- Servir de conseiller dans la prise de décisions stratégiques et tactiques afin de réaliser les buts fixés.[192]

- Fixer les claudications et proposer des solutions.[193]

- Assurer la concordance entre tous les organismes concernés par İnternet et examiner le développement au niveau international puis désigner de nouveaux buts concordant avec les İntêrets de l'Etat.[194]

La création de ce conseil est certes une amélioration très importante pour la Turquie, qui pendant longtemps s'est désintéressé de l'İnternet.

Si les travaux qu'il a accompli sur İnternet sont très réjouissants[195], il est cependant à noter que, cet organisme est totalement public et est loin d'être un organisme de régulation. Il ne dispose aucun pouvoir effectif et ses seules fonctions sont la surveillance et le conseil.

La privatisation partielle (en insérant des fournisseurs d'accès par exemple) du conseil, et l'attribution d'un pouvoir de sanction (même si très limités)

---

[191] Kayıhan İçel, Kitle Haberleşme Hukuku, Beta Yayınevi, Yenilenmiş beşinci Bası,Kasım 2001, İstanbul,p.419.
[192] ibid., p.420.
[193] ibid., p.420.
[194] ibid., p.420.
[195] www.ubak.gov.tr/spam.

concernant les cyber crimes mineurs, aurait permis à la Turquie de rattraper son retard sur la corégulation.

Chapitre II : La régulation Etatique

La répression des crimes sur İnternet se fera de prime abord par les pouvoirs étatiques.

Afin de pouvoir instaurer un arsenal répressif efficace ;

Les Etats doivent dans un premier temps instaurer un systeme de responsabilité prenant en compte tous les intervenants qui sont a l'œuvre dans le fonctionnement du cyberespace (Section I). Et ils doivent dans un deuxième temps adopter leurs règles pénales aux particularités que présentent les crimes commis sur İnternet (Section II).

Section I : la Responsabilité pénale des acteurs de l'İnternet.

La responsabilité pénale des acteurs de l'İnternet est un sujet d'actualité brûlant à travers le monde. En témoignent les actes législatifs comme le *« Teledienstegesetz »* en Allemagne , le « *Communications Decency Act* » aux Etats-Unis et les derniers amendement de loi accomplis en France en l'an 2000 sur la Loi portant sur la Liberté de Communication de 1986 et no86-1067[196].

Comme trop souvent, la Turquie fait figure d'exception.

Il y a un vide juridique dans la réglementation de la responsabilité pénale des acteurs de l'İnternet en Turquie.

Ces acteurs ne peuvent être punis que dans le cadre des règles du droit commun. Donc un acteur d'İnternet ne peut être puni qu'en raison d'un crime qu'il a lui-même commis.

Cela ne pose pas de problème quand il s'agit des internautes et des fournisseurs de contenus.

---

[196] Zeynel T.Kangal "Fransa internet yoluyla işlenen suçlardan doğan ceza sorumluluğu" İÜHFM, Cilt LIX, sene 2001, cilt : 1-2, p. 228.

La situation devient cependant plus délicate quand il s'agit des fournisseurs d'accès, des fournisseurs d'hébergement, des modérateurs Usenet et des fournisseurs d'hypertexte.

Ces derniers ne sont pas les créateurs des informations illicites. Ils ne servent que de support à leur circulation dans le réseau. Quelle sera alors leur position juridique ?

İl n'y a malheureusement pas de réponse nette à cette question en Turquie, par faute d'absence d'une législation traitant de leur responsabilité pénale.

Quoi qu'il en soit, la Turquie légiférera sur ce sujet tôt ou tard. En attendant ces jours, il nous semble intéressant de se lancer dans une tentative de détermination du régime juridique de la responsabilité pénale sur Internet dans le Droit comparé.

Dans ce cadre, nous traiterons de manière intuitive la responsabilité des différents acteurs d'İnternet.

Sous section I : L'İnternaute

L'internaute, comme nous l'avions précédemment évoqué, est l'utilisateur de l'İnternet. Il est celui qui grâce à un ordinateur, navigue sur la toile, se sert d'une messagerie électronique ou consulte les « *newsgroup* » etc. İl est en somme le consommateur des informations contenues sur la toile. Mais le caractère interactif de l'İnternet permet à l'İnternaute d'avoir un comportement contributif. Et c'est à ce moment là qu'il risque de voir sa responsabilité engagée.

En ce qui concerne sa responsabilité du fait de la consommation de l'information, sa responsabilité risque que très difficilement d'être engagé. Mais on peut imaginer le cas de figure dans lequel il stocke dans le disque dure de son ordinateur des images de pornographie dure et ne prend pas les mesures utiles pour qu'un mineur sous sa garde les découvre[197]. Ce manque de diligence pourrait attenter l'intégrité psychique de l'enfant, et pourrait tomber sous le coup de l'article 226 du Nouveau Code Pénal Turc.

---

[197] Morgan Lavanchy, La Responsabilité Délictuelle sur Internet en droit suisse, Université de Neuchâtel – Faculté de droit,Thèse de licence, Session 2002,p.35.
http : // www.droit-technologie.org (21.01.2005).

Pour la responsabilité de l'Internaute d'une déclaration dans un « *news group* » ou dans un forum de discussion non fermé, l'internaute supporte la responsabilité pénale en raison des messages illicites qu'il diffuse.

La responsabilité pénale de l'internaute du fait de l'utilisation de la messagerie électronique n'existe pas du fait que le message électronique soit un moyen de communication privé.

La responsabilité pénale de l'internaute du fait du « *mailbombing* » n'existe pas non plus du fait que cet acte immoral ne soit pas défini en tant que crime dans le code pénal. Une responsabilité civile peut néanmoins être envisagé si la non réception d'un mail, en raison du « *mailbombing* », s'est avérée préjudiciable au propriétaire de la boîte à messagerie électronique.

Sous section II : Les fournisseurs de contenu

Les fournisseurs de contenu sont ceux qui préparent le contenu des publications accessibles sur Internet.[198]

On connaît deux types de fournisseurs de contenu : l'auteur et le « *webmaster* ».

L'auteur crée ou met à disposition sur Internet des informations soit du texte, des images, des sons ou des vidéos.

On est déjà en présence d'un auteur à partir du moment où un cybernaute s'exprime au travers de son site « *web* », d'un « *e-mail* », d'un message de forum de discussion. L'Internet permet à tout en chacun de s'autopublier très facilement et souvent gratuitement.

Le « *webmaster* » est l'administrateur du site « *web* ». Il s'attache surtout à l'aspect technique du site qui doit toujours être accessible aux internautes. Mais le « *webmaster* » est aussi souvent un « *Webdesigner* », soit la personne qui conçoit le site au niveau artistique. C'est le « *webmaster* » qui doit assurer la maintenance et suivi du site Internet[199]. Il faut aussi remarquer que pour les sites non professionnels, l'auteur et le « *webmaster* » sont généralement les mêmes personnes.

---

[198] Sinar, op.cit, p. 41.
[199] Lavanchy, op.cit, p.110.

En Droit allemand, la Loi allemande sur les Téléservices (« *Teledienstsgesetz* ») de 1997[200], prévoit dans son ancien article 5/1 et son nouveau article 8 que le fournisseur de contenu sera tenu responsable d'un contenu illicite que dans le cadre des règle du droit commun. [201]

Cette responsabilité porte sur le contenu (« son contenu ») qu'il lui-même mis en circulation.

Qu'entend on par « son contenu » ? Les motifs de la Loi sur les Téléservices dispose que cette expression englobe les contenus que le fournisseur de contenu a lui-même préparé et ceux préparés par des tiers mais qu'il considère comme les siens.[202]

En Droit français, il n'y a pas de disposition spéciale prévoyant la responsabilité pénale des fournisseurs de contenus.

On se réfère aux règles du droit commun selon lesquelles une personne ne sera pas responsable que d'un crime qu'elle a lui-même commis.

La situation du « *webmaster* »est une situation cependant à part .

Ces derniers seront responsables du contenu illicite d'une information figurant dans le site qu'il administre dans le cadre des règles de la complicité. [203]

On le voit la responsabilité du fournisseur de contenu sur İnternet ne génère pas de question théorique particulière.

De même il n'y a pas de doute aussi qu'en Turquie, selon les règles du droit commun, l'auteur sera responsable en vertu de l'article 20 du nouveau Code Pénal, et le « *Webmaster* » en vertu des règles de la complicité.

Sous section III : Les fournisseurs d'infrastructure.

Les sociétés d'infrastructure sont les sociétés de Télécommunication et les câblodistributeurs qui permettent le transport matériel des informations sur le réseau. İls sont donc des intervenants purement techniques. Toutefois à l'instar des

---

[200] Cette Loi a été promulguée en 1997. En ce sens, l'Allemagne est le premier pays Européen à avoir pensé à légiférer sur la Responsabilité des acteurs de l'İnternet. Cette Loi a cependant été amendée en l'an 2000 , afin de prendre en compte dans le texte de Loi, les principes édictés par la directive no 2000/31 et datant du 8.6.2000 du parlement et du conseil Européen.
Barış Erman, Alman Hukukunda İnternetten kaynaklanan ceza sorumluluğu, İÜHFM, Cilt LIX, sene 2001, cilt : 1-2, p. 208.

[201] Erman ., op.cit, p. 212.

[202] ibid,p.212.

[203] Kangal op.cit,p.231.

fournisseurs d'accès, la mise en cause de leur responsabilité n'est pas exclue lorsqu'ils ont eu connaissance du caractère illicite de certaines informations ayant transité par leur système.

Ainsi dans un jugement du 17 février 1995[204], le tribunal fédéral suisse a condamné un responsable des PTT du chef de complicité de publication obscènes, pour s'être abstenu de mettre fin aux activités d'un info kiosque rose, alors que le ministère public avait attiré son attention sur les pratiques illégales du serveur. Il s'agit du jugement de l'affaire dite du « 156 » ou du «téléphone rose»[205]

En l'espèce, le 7 mai 1991, Monsieur Rosenberg, le directeur général du département des télécommunications des PTT de l'époque, décida l'introduction du télékiosque 156 à titre d'essai, essai qui débuta le 1er octobre 1991. Le système du télékiosque permet à un exploitant de faire écouter des enregistrements sonores. A l'époque en tout cas, il suffisait d'un raccordement téléphonique pour y accéder. Suite à la lettre du Procureur général du canton de Vaud du 11 octobre 1991, le responsable des PTT a su que des publications à caractère pornographique étaient disponibles sur le télékiosque 156, chose dont il devait d'ailleurs se douter. Mais pour les PTT, « des mesures ne pourraient être prises que lorsqu'un jugement pénal définitif et exécutoire rendu contre les abonnés concernés aurait été notifié ». Les PTT ajoutèrent qu'ils « n'ont ni le devoir, ni le droit de soumettre les conversations téléphoniques à des contrôles et que l'abonné est seul responsable de ses messages » : les fournisseurs d'un télékiosque ne pourraient pas être tenus pour responsables des contenus qu'ils véhiculent.

Le Tribunal Fédéral Suisse n'a pas été de cet avis. Il a jugé qu'en continuant à mettre à disposition ce télékiosque, afin de le rentabiliser, Monsieur Rosenberg s'est rendu coupable, au sens de l'art. 25 du Code Pénal Suisse, de complicité de publications obscènes, respectivement de pornographie, car les enregistrements pornographiques étaient accessibles à des jeunes de moins de 16 ans.

La condamnation pénale a surtout tenu au fait que les PTT avaient créé une infrastructure qui rendait les agissements prévisibles et l'avaient maintenue après

---

[204]Thibault Verbiest "Quelle responsabilité pour les acteurs de l'Internet ?" d'après www.juriscom.net/pro/1/resp19990121.htm.(09/12/2003).

[205] "Rosenberg c. Procureur général du canton de Vaud, RO ATF 121 IV 109". D'apres Lavanchy, op.cit,p.40.

avoir été « informés et mis au pied du mur par la lettre du Procureur vaudois ». Il y a donc eu inertie alors qu'il y avait pouvoir et savoir.

Il est à noter que l'office fédéral de la justice a considéré que cette jurisprudence pouvait aussi s'appliquer aux fournisseurs d'accès[206]

Sous section IV : Les fournisseurs d' Accès

Le fournisseur d'accès à Internet offre à ses abonnés, particuliers ou entreprises, une connexion au réseau Internet. En mettant son serveur, connecté en permanence à Internet, à la disposition de ses abonnés, le fournisseur leur permet l'accès à l'ensemble des informations disponibles sur Internet.

Au début de la décennie 1990 le courant mondial qui se dessinait sur la responsabilité des fournisseurs d'accès était la suivante : un fournisseur d'accès qui n'assume aucune responsabilité éditoriale du contenu du site et dont l'intervention est purement technique, sera tenu pour coresponsable des contenus illégaux ou dommageable qu'il permet de relayer que s'il avait ou devait avoir connaissance de la présence de tels contenus sur son réseau.[207]

Néanmoins, en Allemagne; L'affaire *"CompuServe"* de 1995[208] est particulièrement attrayante du fait qu'il a défrayé la chronique et laissé le monde d'Internet en émoi.

En l'espèce, constatant en 1995 que *"CompuServe Information Services GmbH"* - ci-après *"CompuServe GmbH"* - permettait d'accéder à des *"newsgroups"* à caractère illicite, le Ministère public munichois assigna Felix Somm, le directeur de *"CompuServe GmbH"* de l'époque, à couper l'accès à ces groupes de discussion. En fait, Felix Somm n'avait aucun moyen technique de supprimer cet accès. En effet, c'est la maison mère de *"CompuServe GmbH"*, *"CompuServe Inc."*, qui hébergeaient les groupes de discussion sur son *"news server"* et les mettait à disposition de tous les clients de CompuServe des *"newsgroups"* au moyen d'un *"frame relay "*[209]. Felix Somm répercuta donc la demande à *"CompuServe Inc."*, qui bloqua l'accès à quelques *"newsgroups"*. Leur fermeture déclencha une levée de boucliers parmi les

---

[206] Lavanchy, op.cit, p.40.
[207] ibid, p.40.
[208] ibid, p.42.
[209] Un "frame relay" est « protocole de communication utilisé sur les longues distances » « Le Dico du Net » www.net-dico.com/termes/t.html.

abonnés de CompuServe, ce qui amena une vague de résiliation d'abonnements. Il est vrai que si ces groupes de discussion étaient illégaux en Allemagne, la plupart étaient tout à fait licites aux Etats-Unis . En 1996, la firme américaine réouvrit les *"newsgroups"* litigieux - à l'exception des rares groupes au nom manifestement explicite -. Elle estimait qu'elle prenait les mesures qu'on pouvait attendre d'elle en mettant à disposition de chaque abonné le logiciel *"CyberPatrol"*, qui permet à l'internaute de censurer les *newsgroups* de son choix. Conséquemment à la nouvelle attitude de *"CompuServe"*, les autorités pénales bavaroises inculpèrent, en février 1997, Felix Somm pour propagation de messages à caractère pédophile, zoophile et violent. En mai 1998, contre toute attente et même à l'encontre du réquisitoire du Procureur, l'*"Amtsgericht"* de Munich condamna à deux ans de prison avec sursis et à 100.000 Deutschmark d'amende le dirigeant de la filiale germanique pour avoir en connaissance la diffusion des contenus pornographiques en donnant accès à certains *"newsgroups"* et sites *web*. Selon le tribunal, *"CompuServe GmbH"* avait connaissance des contenus illégaux et le blocage de ceux-ci était techniquement possible et raisonnable, considérant qu'il était possible pour *"CompuServe Inc."* de bloquer l'accès aux contenus illicites uniquement pour les abonnés allemands. Si *"CompuServe"* n'a pas agi, ce serait uniquement par peur de perte de profits. En raisonnant sur la base l'art. 2 al. 3 du *"Strafgesetzbuch"* interprété selon l'art. 5 al. 2 du *Teledienstgesetz* (TDG), la cour a donc jugé le dirigeant coauteur de l'infraction.
Ce jugement a provoqué un tollé parmi les professionnels d'Internet. Il est vrai qu'il avait pour conséquence de rendre responsable un fournisseur d'accès à Internet de tout contenu illicite présent sur Internet et d'obliger le fournisseur à des contrôles et filtrages techniquement impossibles. Si l'intention du juge n'était pas mauvaise, elle montre néanmoins son incompréhension du cyberespace. Heureusement, dans son arrêt du 17 novembre 1999, la Cour d'appel de Munich a annulé cette décision de non-sens et acquitté Felix Somm. De l'avis de ce tribunal, l'*"Amtsgericht"* avait confondu à tort *"CompuServe Inc"*. et *"CompuServe GmbH"* : même très liées, elles ne constituent pas moins deux entités juridiques différentes. Et si *"CompuServe Inc."* tenait à disposition de ses abonnés les *"newsgroups"* et aurait pu se voir appliquer l'art. 5 al. 2 du TDG, il n'en était rien de *"CompuServe GmbH"*, qui ne pouvait être défini que comme un simple fournisseur d'accès. L'art. 5 al. 3 du TDG trouvait donc application. Et selon cette disposition, le prestataire de services qui ne donne que l'accès à des contenus illicites ne peut être tenu pour responsable. Même en

application de l'art. 5 al. 2 du TDG, le dirigeant n'aurait d'ailleurs pas dû être condamné, car « le blocage par un fournisseur d'accès allemand d'informations de nature pornographique provenant des Etats-Unis n'était pas raisonnablement possible».

Un amendement a été cependant opéré en 2001 dans la Loi allemande sur les Téléservices. Cet amendement a instauré de nouveaux principes pour la responsabilité pénale des fournisseurs d'accès sur Internet[210]. Selon ces nouveaux principes, les conditions de la responsabilité pénale des fournisseurs d'accès sont les suivantes :

Le fournisseur d'accès ne sera pas responsable du contenu illicite des informations qu'il stocke automatiquement et pour une courte durée dans le disque dur de son ordinateur tant qu'il n'effectue pas une intervention consciente à la circulation de ces informations sur le réseau.

Ainsi, afin de ne pas voir sa responsabilité engagée, le fournisseur d'accès ne doit pas être à l'origine de la transmission des informations illicites, ne doit pas sélectionner leur destinataire, ne doit pas selectionner ni modifier le contenu de ces informations.[211]

Les amendements accomplis dans la Loi allemande vise à restreindre la responsabilité pénale du fournisseur d'accès, tant qu'il se limite au transport des données. Si, celui ci se contente d'un rôle passif, s'il reste neutre, il n'encourera pas le risque de voir sa responsabilité engagée.

En Droit français, les règles de droit commun s'avérant insuffisantes pour régir la responsabilité des fournisseurs d'accès, la Loi sur la Liberté de Communication a été amendée ,en l'an 2000, dans ce but.[212]

Cette Loi traite la responsabilité des fournisseurs d'accès dans son article 43-10. Notons que cet article ne prévoit que la responsabilité delictuelle de celui-ci. Il n'y aucune disposition dans cette loi traitant de leur responsabilité pénale. Cette abscence de disposition s'explique en droit français, par la non-attribution de responsabilité pénale aux fournisseurs d'accès. Et cela s'explique par deux raisons :

- Les fournisseurs d'accès ne peuvent pas être tenus responsable d'un contenu illicite dont il ignorait l'existence jusqu'à ce que le crime soit révélé ;

---

[210] Erman,op.cit, p.216.
[211] ibid, p.216.
[212] Kangal, op.cit, p.233.

Ces acteurs ne peuvent pas être considéré comme le complice de l'auteur principal du crime car le droit pénal français recherche que la complicité soit opérée en même temps que la réalisation du crime. Or la mise en ligne des contenus illicites s'effectue avant qu'un lien ne soit établi, c'est à dire, avant même la présence du fournisseur d'accès.

- Le fournisseur d'accès n'est pas capable d'agir intentionellement. En droit français afin que quelqu'un soit considéré complice d'un crime, il faut que ce dernier ait agi intentionellement .[213]

En Droit américain, c'est la "*Communication Decency Act*" qui traite de la responsabilité pénale des fournisseurs d'accés.[214]

Ce texte législatif exonère les prestataires techniques de toute responsabilité pour le contenu de tiers et cela sans condition, sauf si une instance judiciaire l'a mis auparavant au courant du contenu illicite des informations qu'il permet de circuler sur le réseau.

L'expression "prestataire technique" recouvre les fournisseurs d'accès.[215]

Nous pouvons dans ce cadre citer l'exemple d'une jurisprudence emise par un tribunal américain.

Dans l'affaire "*Zeran v. America Online (AOL)*" [216], le demandeur s'était plusieurs fois plaint auprès d' "*AOL*" de messages diffamatoires postés sur un des forums de discussion par un internaute anonyme. Celui ci s'obstina à ne pas supprimer les messages litigieux. La cause alla jusqu'à la Cour Suprême. "*Zeran*" reprochait à "*AOL*" sa non réaction, notamment le fait de ne pas avoir prévenu les usagers des ses services que les "*postings*" étaient erronés. Mais, la cour confirma les avis des cours inférieurs et "*AOL*" échappa à toute responsabilité. Les cours concernées se sont basées sur l'idée ue les fournisseurs d'accès risquerait de voir sa responsabilitée en gagée, s'il ne traitait pas le cas avec une grande attention. Or, les plaintes des usagers d'internet seront tellement fréquentes- par rapport à celles qui peuvent arriver sur le bureau d'un rédacteur de magazine- que le fournisseur sera vite submergé et deviendrait une cible trop facile ou alors supprimerait sans autres tout

---

[213] ibid, p.232-234.
[214] Verbiest, op.cit.
[215] ibid.
[216] "*Kenneth M.Zeran V.AOL,Inc.,U.S. Supreme Court, Cert. Pet. 97-1488*" d'après Thibault Verbiest, op.cit.

message douteux, contrevenant ainsi au "*Free Speech*". Si "AOL" avait décidé d'agir, il aurait été simplement considéré comme un "bon samaritain".[217]

Cet arrêt valable pour n'importe quel fournisseur, instaure un régime d'immunité quasi totale qui est tout bonnement et visiblement innaceptable vis à vis du mode de pensée juridique européen. Les principes se dégageant peuvent certes se justifier pour les fournisseurs d'accès , mais en aucun cas pour l'hébergeur, comme on le verra tout de suite.

Sous section V : Les fournisseurs d'Hébergement

Les fournisseurs d'hébergement prêtent de l'espace mémoire de leurs ordinateurs pour que l'utilisateur puisse y loger un site web. De nombreuses sociétés commerciales et personnes publiques (universités, établissements publics) offrent d'héberger, en général contre rémunération, des pages Web sur leurs propres serveurs. L'hébergeur agit donc comme un bailleur : Il loue un emplacement sur le Web ou le locataire pourra publier ce qu'il veut.[218] Lorsqu'un fournisseur d'hébergement attribue une adresse URL à un nouveau site, il a théoriquement le pouvoir de contrôler le contenu des fichiers des pages web qui lui sont remis. Dans ce cas ayant constaté que l'activité projeté est illégale ou dommageable et que le fournisseur d'accès accepte néanmoins d'héberger le site, sa responsabilité devra être engagée.

En Droit allemand, la Loi allemande sur les Téléservices prévoit dans son ancien article 5/2, et son nouveau article 8/2, une disposition spéciale pour la responsabilité pénale du fournisseur d'hébergement. Ce dernier ne peut être responsable du contenu illicite qu'il héberge qu'à certaines conditions : S'il est au courant de l'illicéité du message et que s'il en son pouvoir d'arrêter la publication. Sur ce, la responsabilité pénale des fournisseurs d'hébergement reste exceptionelle.

Cependant avec l'amendement en 2001, le législateur allemand, tout en restant fidèle au même principe, a imposé des charges supplémentaires au fournisseur d'hébergement.[219]

---

[217] Jougleux,op.cit,p.145.
[218] Jougleux, op.cit,p.145.
[219] Erman, op.cit,p.221.

Effectivement, le législateur allemand a refusé d'attribuer au fournisseur d'hébergement une obligation de contrôle permanente des informations, sachant que la pratique de ce contrôle est impossible face aux miliers de message qui transitent quotidiennement les serveurs de celui-ci. Cependant il a prévu une situation dans laquelle le fournisseur ne peut pas échapper à la responsabilité pénale : c'est le cas où celui-ci est mis au courant de l'illicéité des informations qu'il héberge. Mais cette mise au courant de l'hébergeur doit présenter certaines particularités : elle doit être positive, c'est-à-dire qu'elle doit être opérée soit par un tribunal, soit par une administration publique.[220]

Dans le cas de la France, ne disposant pas de textes législatifs sur la responsabilité des acteurs d'Internet jusqu'en 2000, les tribunaux français ont tenté de résoudre le problème en comparant le fournisseur d'hébergement au responsable éditorial exerçant un contrôle sur le contenu du service.

L'affaire Estelle Hallyday[221] fournit un bon exemple à ce sujet .

Notons que cette affaire relève de la responsabilité delictuelle du fournisseur d'hébergement. Nous la considèrons importante, car elle a été une des raisons de l'amendement de la Loi sur la Liberté de Communication en l'an 2000, régissant également la reponsabilité pénale de ces acteurs.

En l'espèce, au début de 1998, Estelle Hallyday constate la présence d'une vingtaine de photographies privées la représentant partiellement ou complètement nue sur le site « *http://www.altern.org/silversurfer* ». Faute de pouvoir identifier le propriétaire du site, le mannequin assigne le gestionnaire et représentant du service d'hébergement « *Altern.org* »,Valentin Lacambre, en référé devant le Tribunal de Grande Instance de Paris, en invoquant une violation de son droit à l'image et de l'intimité de sa vie privée. Elle demande des dommages et intérêts et l'interdiction de poursuivre la diffusion de ces photographies. La violation des droits d'Estelle Hallyday n'est pas contestée. Dans l'ordonnance de référé, le juge estime que « le fournisseur d'hébergement a l'obligation de veiller à la bonne moralité de ceux qu'il héberge, au respect par ceux-ci des règles déontologiques régissant le web et au respect par eux des lois et des règlements et des droits des tiers ». Il précise que l'hébergeur peut aller « vérifier le contenu du site qu'il héberge » et ainsi faire cesser les atteintes aux droits des tiers. Il ajoute que « pour pouvoir s'exonérer de sa

[220] Erman,op.cit,p.223
[221] Lavanchy , op.cit, p.61-64

responsabilité, [le fournisseur] devra donc justifier du respect des obligations mises à sa charge, spécialement quant à l'information de l'hébergé sur son obligation de respecter les droits de la personnalité, le droit des auteurs, des propriétaires de marques, la réalité des vérifications qu'il aura opérées au besoin par des sondages, et des diligences qu'il aura accomplies dès la révélation d'une atteinte aux droits des tiers pour faire cesser cette atteinte ».

Le juge n'accorde pas les dommages-intérêts que la demanderesse sollicite et l'invite à saisir le juge du fond, jugeant que la problématique de la responsabilité des fournisseurs d'hébergement et la détermination des causes d'exonération susceptibles d'être invoquées, dépasse ses compétences. Par contre, vu l'urgence, il enjoint Valentin Lacambre, « sous astreinte de 100.000 francs par jour, de mettre en oeuvre les moyens de nature à rendre impossible toute diffusion des clichés photographiques en cause à partir de l'un des sites qu'il héberge ».

Les parties se retrouvent devant la Cour d'appel de Paris. Celle-ci infirme l'ordonnance quant aux mesures d'interdiction, au motif qu'elles étaient inutiles, dans la mesure où les photographies avaient été retirées du site, et qu'elles étaient, au surplus, non définies et difficiles d'exécution. Mais la cour définit surtout le rôle, juridiquement parlant, du fournisseur d'hébergement, qui, en stockant des contenus « qui n'ont pas le caractère de correspondances privées, [...] excède manifestement le rôle technique d'un simple transmetteur d'informations et doit, d'évidence, assumer à l'égard des tiers aux droits desquels il serait porté atteinte dans de telles circonstances, les conséquences d'une activité qu'il a, de propos délibérés, entrepris d'exercer dans les conditions susvisées et qui, contrairement à ce qu'il prétend, est rémunératrice et revêt une ampleur que lui-même revendique ». Le juge considère ainsi que la diffusion des photographies dans les conditions de l'espèce engage manifestement la responsabilité de Valentin Lacambre et le condamne à payer à Madame Hallyday la somme de 300.000 FF à titre de dommages-intérêts.

L'ordonnance du 9 juin 1998 a été un véritable électrochoc.

Le problème est que le contrôle systématique - a priori ou a posteriori - de milliers de pages web est techniquement impossible. Il est en plus socialement, économiquement et juridiquement inacceptable.

Prenant le contre-sens d'une tendance prônant la responsabilité reduite des prestataires techniques, cette ordonnance a grandement indigné les professionnels d'Internet et a secoué les politiques français, qui ont très vite délivré

des projets d'amendement ou de loi , tel que l'amendement de laLoi sur la Liberté de Communication de 1986 .

Celui-ci, dans son article 43-8, s'approchant du modèle allemand, a réduit les possibilités de mise en jeu de la responsabilité pénale des hébergeurs aux cas où, "en connaissance de cause, ils n'ont pas agi avec promptitude pour faire cesser la diffusion d'une information ou d'une activité dont ils ne pouvaient ignorer le caractère illicite".

Là aussi l'hébergeur est considéré comme ne pouvant ignorer le caractère illicite de la diffusion que s'il en a été averti par une administration judiciaire.[222]

Sous section VI : Le modérateur Usenet (*newsgroups)* ou d'un forum de discussion

Les services tels que « *Usenet* » sont les supports de l'essentiel du trafic sur Internet. L' « *Usenet* » est formé essentiellement à partir de groupes de nouvelles, groupes de discussion thématiques, classés selon une structure hiérarchique. Ils offrent un moyen de communication et d'échange d'informations remarquable, en permettant à leurs abonnés de lire et de publier des messages, notamment de poser des questions ou d'y répondre.[223]

Il existe des groupes de discussion pour tous les goûts.

Une partie des *newsgroups* sont modérés : avant d'être disponibles, les articles sont contrôlés par un modérateur qui choisira ou non de les diffuser. Une telle pratique permet de vérifier la conformité des messages avec les normes régissant le *newsgroup*. Elle permet surtout d'éviter les messages risquant de mettre le feu aux poudres ou les messages sans valeur ou sans rapport avec le thème, en particulier les *spams* : en d'autres termes, le modérateur enlève le "bruit".

Il convient alors de se demander quelle sorte de responsabilité pourrait on infliger au modérateur, s'il laisse passer des messages visiblement illicites.

Les réflexions jurisprudentielles sur la responsabilité du modérateur des newsgroups et les forums de discussion se rapprochent en général de celles de la responsabilité du directeur éditorial du journal.

---

[222] Kangal, op cit, p.237.
[223] Lavanchy,op.cit,p.103.

Nous pouvons citer ici parmi les affaire les plus célèbres , "l'affaire Aftonbladet.", jugé par le tribunal de Stockholm.[224]

Dans l'affaire Aftonbladet en l'espèce;

En octobre 2000, plusieurs *"postings"* au contenu anti-sémite sont disponibles sur le forum de discussion du site d'Aftonbladet, journal de renom suédois. Les messages restent plusieurs jours sur ce forum ouvert, mais modéré. Poursuivi pour provocation à la haine raciale, le directeur éditorial du journal est condamné par un tribunal de Stockholm, le 7 mars 2002. Le modérateur du forum aurait dû censurer les *"postings"* litigieux.

Nous pouvons aussi citer un des premiers arrêt rendu par un tribunal turc, la quatrième cour d'assise d'İstanbul, portant sur la responsabilité pénale d'un moderateur d'un forum de discussion.

En l'espèce, l'administrateur d'un site de forum de discussion travaillant dans une entreprise de fournisseurs d'accès à İnternet basée a İstanbul (« *Superonline* »), fut jugé pour la violation de l'article 159 du Code Pénal Turc, pour ne pas avoir mis fin à la diffusion d'un message dont le contenu portait atteinte à la respectabilité de la République Turque, des forces Militaires Turques, des Forces Turques pour la Prévention de la Sécurité, et enfin de la personnalité morale de la Justice.

Le titulaire du message dont le pseudonyme était « un humain » fut introuvable.

L'administrateur du site de forum était au courant du contenu illicite du message, car un autre adhérant au forum lui en avait averti. Malgré cette mise en garde, l'administrateur négligea le retrait du message qui fut diffusé tout au long d'une semaine, le temps nécessaire pour que le procureur de la République d' İstanbul fût mis au courant. Ce dernier assigna l'administrateur du forum à la quatrième cour d'assise qui décida à 40 mois de prison, le 27 mars 2001, à la fin du jugement.

Cette décision fut menée à la Cour de Cassation qui l'infirma en raison de sa formation au bout d'une investigation incomplète : selon la Cour de Cassation , la cour d'assise avait négligé de constater à l'aide du rapport d'un comité d'experts, si l'entreprise « *Superonline* » fournissait des services d'accès ou d'hébergement à İnternet ou les deux à la fois, si le forum en question était bien administré par une

---

[224] ibid,p.104.

personne physique et s'il était en son pouvoir de cesser la diffusion du message en question.

Sur ce, la quatrième cour d'assise d'Istanbul fût resaisi pour le jugement de cette affaire. Celle-ci insista sur sa première décision.

L'affaire fût renvoyé à la Cour de Cassation, le jugement fût cette fois ci repris dans le conseil général pénal qui infirma aussi la décision, demandant sa reconsidération en vue de la Loi no 4771 promulguée le 3.8.2002. Prévoyant des amendements dans plusieurs lois y compris le code pénal et son article 159.

La cour d'assise reforma enfin son jugement, décida l'acquittement de l'administrateur du forum, pour l'absence d'intention dans la formation du crime.[225]

En partant de ces deux arrêts nous pouvons dégager ici les conditions selonlesquelles la responsabilité d'un modérateur de forum de discussion risque d'être engagée :

-Un message à contenu illicite devra être déposé sur les serveurs du forum de discussion / ou du service « Usenet »

- l'administrateur doit être au courant du message et de son contenu
- il doit être en son pouvoir de mettre fin à la diffusion du message
- il ne doit pas mettre fin à la diffusion

Sous section VII : Le gérant d'un outil de recherche.

Les moteurs de recherche sont l'armature de l'İnternet, l'intermédiaire obligé de l'İnternet dans la plupart des cas. Les services qu'ils fournissent ont constitué l'un des éléments essentiels au développement d'Internet en permettant la réunion des chercheurs d'informations et des donneurs d'informations.[226]

Sans les instruments de localisation de l'information, nul espoir de tomber par hasard sur la page courue si l'internaute « voyage » sans adresse précise. Il ne faut pas oublier qu'il existe des milliards de pages "*web*" et qu'elles ont la fâcheuse tendance d'être en perpétuel mouvement.

---

[225] Les réferences en turc de cet arrêt sont :
"İstanbul 4. Ağır Ceza Mahkemesi 24.4.2003 tarih, 2003/438 E., 2003/88 K."
[226] Lavanchy,op.cit,p.80.

Sans les instruments de localisation de l'information, un site "*web*" serait invisible sur la toile, sauf publicité. Pour survivre, un site doit être répertorié dans un outil de recherche.

L'outil de recherche servant à tout, il peut être utilisé afin d'accéder à des œuvres contrefaisantes, à des messages délictueux, contraire à la dignité humaine. On a vu l'importance jouée par certains mots clés tel que « *Warez* », certains mots clé renvoient par nature à un site Web contenant sans doute un élément délictueux. Se faisant, il facilite en quelque sorte la réalisation de certaines infractions dans le cyberespace.

En est il responsable ? On serait tenté de répondre que comme le fournisseur d'accès, il ne fait que jouer le rôle d'intermédiaire sans avoir la possibilité d'influer sur les événements. Or il est techniquement possible d'interdire certaines recherches. Donc il devra être tenu comme responsable pour avoir facilité la découverte d'un contenu illicite.

D'ailleurs l'Autriche et les Etats Unis n'ont pas tardé à prendre des précautions à ce sujet.

Le premier texte en vigueur traitant de la responsabilité des outils de recherche a été le "*Digital Millenium Copyright Act*".[227] L'article 512d de cette loi aborde la responsabilité, pour complicité de violation du droit d'auteur, des fournisseurs de services qui ont amené les internautes à un contenu ou une activité contrefaisants "en utilisant les outils de localisation, en l'incluant au répertoire, à l'index, aux références, ou lien hypertexte" . Les conditions d'exonération sont les mêmes que celles de l'hébergeur. Plus précisément, le prestataire :

• ne doit pas avoir une connaissance effective - ou de fait - du contenu ou de l'activité violant le droit d'auteur et ne doit pas être conscient de faits ou circonstances qui rendraient le caractère contrefaisant apparent ;

• doit promptement retirer les informations en question ou en bloquer l'accès, s'il a la connaissance ou la conscience décrites au premier point ;

• ne doit pas percevoir un avantage financier provenant directement de l'activité contrefaisante, dans le cas où le fournisseur a le droit et la capacité de contrôler cette activité ;

• et doit respecter les règles de procédure de notification et contre-notification vues précédemment.

---

[227] ibid.,p.81.

L'Autriche est un autre pays ayant prévu dans ses textes législatifs la responsabilité du gérant des outils de recherche.[228]

Dans le "*E-Commerce-Gesetz*" autrichien, l'art. 14 al. 1 prévoit les mêmes exceptions de responsabilité pour les moteurs de recherche et autres moyens électroniques de recherche d'informations étrangères que pour les fournisseurs d'accès. Le prestataire n'est donc pas responsable s'il n'est pas à l'origine de la transmission des informations demandées, ne sélectionne pas le destinataire des informations demandées et ne sélectionne, ni ne modifie les informations demandées. L'alinéa second de l'art. 14 prévoit que l'alinéa 1er ne s'applique pas lorsque le destinataire du service agit sous l'autorité ou le contrôle de l'outil de recherche.
Mais l'important est que les conditions d'exonérations sont typiquement celles d'un fournisseur d'accès.

Section II : Les caractéristiques relatifs à la procédure pénale.

Le caractère extra territoriale du réseau attribue certaines particularités aux crimes commis sur İnternet auxquels les systèmes repressifs doivent y être sensibles.

Sous section I : Le détermination du lieu de la réalisation du crime et du droit pénal applicable.

La détermination du lieu de la réalisation d'un crime est importante car elle nous permet de savoir quel tribunal sera compétent pour la poursuite et le jugement de ce crime.

Cela ne présente pas de particularité pour les crimes dont l'acte et le résultat sont simultanés. Or les crimes commis sur İnternet sont en général des crimes de distance. C'est-à-dire que l'acte incriminé et le résultat dommageable qui constituent l'élément matériel du crime se réalisent dans deux endroits différents.[229]

---

[228] ibid.,p.82.
[229] Dönmezer Sulhi – Erman Sahir, Nazari ve Tatbiki Ceza Hukuku, Cilt I, 12.Bası, İstanbul, Beta Yayınevi, 1997 , p.243.

Dés lors se pose le problème de la détermination du lieu de réalisation du crime.

Plusieurs théories se mettent alors au service pour déterminer ce lieu.[230]

Le premier est la théorie accordant la priorité à l'acte. Selon cette théorie, le lieu de réalisation du crime est le lieu où l'acte est accompli.

Le deuxième est la théorie accordant la priorité au résultat. Cette théorie affirme que le lieu de réalisation du crime est le lieu où le résultat de l'acte s'est réalisé.

La troisième théorie est la théorie hybride[231], elle est aussi appelée la théorie de l'ubiquité[232]. Selon cette théorie, le crime est commis aux lieux où l'acte a été réalisé, où il continue, et là où le résultat de l'acte est survenu.

Il faut noter que cette dernière théorie est celle acceptée dans la doctrine du droit pénal et dans les congrès internationaux comme la Réunion de Cambridge de 1931 de l'Institut du Droit International Public et la conférence de Varsovie sur l'Unification du Droit pénal de 1927.[233]

La situation ne pose pas de problème quand l'acte incriminé et le résultat dommageable du crime se réalisent à l'intérieur du même pays. Elle devient cependant plus fourchue quand ces deux se réalisent dans deux pays différents : la question relève alors du droit pénal international.

Alors qu'hier on faisait exceptionnellement appel au droit pénal international, aujourd'hui avec la généralisation de l'Internet dans tous les pays de la planète, cela est devenu quotidien. Etant donné qu'une publication sur Internet peut être interceptée par tous les pays du monde, dans le cas d'un message illicite, l'Internet devient susceptible de se voir appliquer tous les droits de la planète, selon la théorie hybride. Et c'est ce fait qui pose la véritable difficulté.

En cas d'infraction internationale, c'est-à-dire d'infraction dont les éléments constitutifs ne peuvent être rattachés à un territoire unique[234], le droit pénal international se contente de renvoyer aux lois internes qui déterminent elles même

---

[230] ibid, p.243.
[231] ibid, p.244.
[232] De Marco Estelle, Le Droit Pénal Applicable sur Internet, Université de Montpellier 1, Institut de Recherche et d'Etudes pour le Traitement de l'Information Juridique, Mémoire de D.E.A. Informatique et Droit, Annee de soutenance 1998, p.14 .
[233] Dönmezer-Erman, op.cit,cilt I, s.244.
[234] De Marco,op.cit, p.13.

leur champ d'application territoriale, se contentant de dire si elle a compétence ou non pour régir un fait[235]. İl convient donc d'examiner ce que les droits pénaux internes proposent.

En Turquie, la Loi pénale turque s'applique sur le territoire turc et par extension de compétence à certaines infractions commise hors de la Turquie mais réputées l'avoir été en Turquie[236].

La question à étudier est alors celle de savoir selon quels critères une infraction est localisée en Turquie.

A. La Localisation nationale d'infraction internationale

En effet, l'alinéa premier de l'article 3 de l'ancien Code Pénal Turc et l'article 8 du nouveau Code Pénal Turc dispose que la Loi pénale Turque est applicable à toutes les infractions commises sur le territoire turc.

Le nouveau Code Pénal apporte une précision quand à la détermination de la localisation de l'infraction (deuxième phrase du premier alinéa) : l'infraction est réputée commise en Turquie dés lors que la totalité ou une partie de l'acte, ou le résultat a eu lieu en Turquie.

Donc le droit pénal turc est applicable à la grande majorité des infractions commises sur İnternet.

B. La localisation nationale par extension

Notre droit national a aussi une application extraterritoriale. Le droit turc s'applique en dehors du territoire turc dans certains cas .

İl est applicable en vertu de deux types de compétences complémentaire : La compétence personnelle et la compétence réelle.

La compétence personnelle est déterminée par la nationalité de l'auteur (compétence personnelle active) ou de la victime de l'infraction considérée (compétence personnelle passive)[237]

---

[235] Dönmezer -Erman, op.cit, Cilt III, s.346.

[236] l'article 8 du Nouveau Code Pénale Turc.

[237] Dönmezer-Erman,op.cit, cilt I, p.250-251.

Les règles relatives à la compétence personelle sont prévues par les articles 5,6,7 de l'ancien code pénal turc et les articles 11 et 12 du nouveau code pénal.

Elles permettent de faire tomber sous le coup de la Loi turque toute infraction dont l'auteur ou la victime est de nationalité turque, et ceci avec les nuances selon la gravité de l'infraction.

La compétence réelle est déterminée par la nature de l'infraction : dans ce cas la Loi Turque s'applique à des infractions qui n'ont aucun lien avec le territoire turc et qui n'implique aucune personne de nationalité turc avec pour seule critère de compétence la nature de l'infraction. Le droit pénal turc a ainsi compétence pour régir les crimes et les délits qualifiés de génocide, d'atteintes aux interêts fondamentaux de la Nation, de torture, de prostitution, de falsification et de contrefaçon des pièces de monnaie et de billet de banques et d'effet publics, du sceau de l'Etat et de tous les autres crimes exhaustivement cités dans l'article 13 du nouveau Code Pénal et de l'article 4 de l'ancien Code Pénal.

Ce nécessaire dévéloppement sur le champ d'application du droit pénal turc nous démontre que celui-ci est applicable à l'ensemble des infractions commises sur le réseau, dés l'instant que la République turque s'estime concernée par les actes en question.

Sous section II : La détermination du tribunal compétent

Le principe général dans le système turc est la compétence du tribunal du lieu où l'infraction a été commise. Une infraction peut être considérée comme commise que si son resultat dommageable se produit.

Les infractions d'Internet, étant en général des crimes de distance, il peut arriver que l'acte incriminé et son résultat dommageable surviennent dans deux pays differents.

Nous avons vu précédemment que la loi penale turque devient applicable dés lors que l'acte ou le résultat du crime se produit en Turquie.

Quel sera alors, le tribunal compétent au jugement du crime, si l'acte incriminé se produit en Turquie et le résultat dommageable à l'étranger ?

Nous pensons que dans ce cas, le tribunal du lieu où l'acte incriminé est réalisé, sera compétent. Si ce lieu est indéterminable, le tribunal du lieu où l'auteur du crime est saisi, ou s'il n'est pas saisi le tribunal du lieu de son domicile devra être compétent. On doit se réfèrer ici aux régles générales de la procédure pénale notamment à l'article 10 de l'ancien code de procédure pénale et aux articles 13 et 14 du nouveau code de procédure pénale.

Dans le cas d'un message illicite provenant de l'étranger mais étant perceptible par toutes les villes de la Turquie, il faudra considérer comme compétents tous les tribunaux d'où cette message pourra être perçu. Et en cas d'atteinte aux droits d'une personne, il faudra considérer comme compétent le tribunal du lieu de domicile.

Sous section III : La détermination du moment de la réalisation du crime.

Il existe aussi des particularités quand à la détermination du moment où le crime est commis. La diffusion ne produisant pas ses effets simultanément dans tous les pays du monde, il convient de se demander, quand nous pouvons considérer le crime comme étant commis. Cela est essentiel, car elle marquera également le commencement des durées de prescriptions.

En Turquie, un crime est considéré comme étant commis au moment même où le resultat dommageable est survenu.[238]

Alors il est évident qu'un problème risque de se poser si ce résultat dommageable se produit en dehors du territoire turc. Comment va-t-on pouvoir déterminer le moment de réalisation du crime ?

Nous pensons que le moment de réalisation du crime est le moment où le résultat dommageable se produit à l'étranger. Pour les crimes restées au stade de la tentation, c'est le moment où le dernier acte incriminé s'est reproduit en Turquie.

Sous section IV : Les règles de procédures pouvant être appliquées aux cyber crimes.

Les techniques de jugement varieront en fonction du crime commis.

---

[238] Dönmezer-Erman, op.cit, cilt III, p.258.

Si le cyber crimes vont à l' encontre de l'Etat ou des administrations publiques, il serait adéquat de se référer, aux règles générales de procédure pénale.

En ce qui concerne les crimes un peu moins graves, les moyens d'actions civiles, de paiement préalable, d'ordonnance pénale du juge de paix pourront être appliqué a l'İnternet. [239]

Sous section V : La mise en place de sanctions adaptées à l'İnternet.

Diverses peines complémentaires ou alternatives sont envisageables. La première de loin la plus évidente consiste à ordonner la publication de la décision de justice sur la toile et de préférence sur le site sur lequel s'est commis l'infraction.

Cette première sanction à fin préventive et pédagogique mais aussi répressive peut être accompagnée de l'obligation de créer un lien hypertexte pointant vers un organisme officiel ou vers le site de la victime.

D'autres sanctions sont envisageables : une des plus originales consiste à interdire le délinquant de se connecter au réseau. Cette privation de l'Internet peut se faire pour une durée limitée et doit être compris strictement comme l'interdiction faite à l'individu de prendre un abonnement chez un fournisseur d'accès Internet, la non application de cette sanction pouvant occasionner la disparition du sursis par exemple. Cette sanction a déjà été appliqués aux Etats-Unis. Les règles pénales étant d'interprétation stricte, cette nouvelle interdiction ne peut être prononcée par un juge turc tant qu'elle n'est pas consacrée par le législateur.[240]

D'autres sanctions également envisageables, l'individu peut être employé par une association s'occupant de la recherche et de la dénonciation des sites pédophiles, il peut lui être imposé d'assurer le contrôle d'un forum de discussion, un hacker se verra obligé d'assurer la sécurité du système informatique de la commune…

---

[239] « İnternet ve Hukuk » www.superonline.com/hukuk/hukuk.htm (01.09.2004).

[240] ibid.

Chapitre III : La Régulation Internationale : La Convention Européenne sur la Cybercriminalité.

Nous avions précédemment évoqué brièvement que tous les droits de la planète n'incriminaient pas les mêmes faits ou qu'ils les réprimaient de manière différente. En effet c'est la différence entre les conceptions étatiques de la liberté étatique qui pose la réelle difficulté. Marcelin-Taupenas avait bien raison d'affirmer dans une phrase désormais célèbre[241] : « Le Droit présente des disparités quand à la liberté d'expression, le contenu d'un message transporté sur Internet peut être jugé innocent ici, indécent là, criminel ailleurs ».

Tenter de résorber ces disparités ne relève plus de l'ordre technique mais de l'ordre moral : c'est la souveraineté des Etats qui est mise en cause.

Ces conflits de Lois, externes et internes provoquent un affaiblissement marqué des principes du droit pénal.

La solution pour combattre la multiplicité des lois applicables sur Internet est de déterminer un droit unique qui s'y substituerait.

Aujourd'hui, les Etats réalisent qu'Internet concerne chacun d'entre eux au même titre que leur voisin et ainsi l'obstacle majeur au développement du droit international pénal, la souveraineté des Etats, commence à se soulever. Un Droit veritablement international commence à s'élaborer progressivement. Et la Convention Européenne sur la Cybercriminalité en fournit un bon exemple.

Cette convention fût signée en 2001 en Hongrie à Budapest. 31 Etats signèrent cette convention le même jour. Le 02.05.2002 ce nombre monta à 32 Etats.

Parmi les Etats adhérents quatre sont en dehors de l'Europe : les Etats-Unis, le Canada, le Japon et l'Afrique du Sud.

Cette convention vise de mener une politique pénale commune afin de protéger la société de la cybercriminalité ; l'adoption de pouvoirs suffisants pour permettre une lutte efficace contre ces infractions pénales en facilitant la détection, l'investigation et la poursuite tant au plan national qu'au niveau international, et enfin de réaliser une coopération internationale accrue, rapide et efficace pour lutter contre la cyber criminalité.

---

[241] Marcelin Taupenas Sabine, "Droit de l'Informatique" supplement no 74, lamy, octobre 1995, p.1 d'après De Marco Estelle,op.cit, p.30.

Section I : Les principes généraux édictés par la Convention Européenne sur la Cybercriminalité.

La Convention Européenne sur la Cybercriminalité est construite sur quatre principes généraux et directifs. [242]

Le premier principe édicté par la Convention Européenne sur la Cybercriminalité est la garantie d'un équilibre adéquat entre les intérêts de l'action répressive et les Droits de l'homme fondamentaux tels que la liberté d'expression, le droit de ne pas être inquiété pour ses opinions et le droit au respect de la vie privée.

Le deuxième principe est l'élaboration d'un standard minimum commun dans l'incrimination des infractions commises par l'intermédiaire d'un système informatique.

Le troisième principe est l'illégalité de l'acte. La convention accentue l'élément d'illégalité pour tous les crimes prévus dans le texte.

Enfin le quatrième principe est l'intentionnalité du crime : tous les cybercrimes évoqués dans la convention doivent être obligatoirement des crimes intentionnelle.

Section II : Les dispositions relatives au droit pénal dans la Convention.

La Convention prévoit quatre types de crimes : les infractions contre la confidentialité, l'intégrité, la disponibilité des données et des systèmes informatiques ; les infractions informatiques ; les infractions se rapportant au contenu, et, les infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes.

---

[242] Kayıhan İçel, "Avrupa Konseyi Siber Suç Politikasının Ana İlkeleri" İÜHFM, Cilt LIX, sene 2001, cilt : 1-2, p.3.

Sous Section I : Les infractions contre la confidentialité, l'intégrité, la disponibilité des données et des systèmes informatiques

L'objectif de cette partie de la Convention est l'élaboration d'un standard minimum commun pour prévenir et contrôler ces crimes.

Les crimes figurant dans la Convention doivent être commis de manière illégale. En cas de l'existence des raisons de légalité comme le consentement de la victime ou la défense légitime ou la nécessité, l'acte ne pourra pas être incriminé et poursuivi.[243]

A. L'article 2 :« L'Accès İllégal »

« Chaque partie adopte les mesures législatives et autres qui se révèlent nécessaire 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'İntention d'obtenir de données informatiques ou dans une autre intention délictueuse, ou soit en relation avec un système informatique connecté a un autre système informatique. »

L'accès illégal à un système informatique est incriminé ici

L'accès illégal comprend ici les menaces et les attaques à la sécurité du système informatique ainsi qu'aux données que celui ci contient.

Les délits tels que le « *hacking* » et le « *cracking* » y sont visés.

Ce type d'accès illégale pourrait aboutir à l'atteinte au secret de la vie privée, l'utilisation gratuite d'un système informatique qui normalement est rémunéré ou peut inciter les hackers aux crimes plus dangereux tels que la fraude et la falsification informatique.

L' « accès » comprend les accès à une partie ou à tout le système informatique. Cet accès peut s'opérer par les réseaux publics de télécommunications, par le réseau interne à une organisation, ou par un réseau comme « l'intranet ».

---

[243] Füsun Sokullu Akıncı, "Avrupa Konseyi Siber Suç Sözleşmesinde Yer Alan Maddi Ceza Hukukuna ilişkin Düzenlemeler ve özellikle Çocuk Pornografisi" İÜHFM Cilt LIX; Sene 2001, sayı 1-2 , p.11.

L'accès doit absolument être illégale. Un accès accompli avec le consentement de la victime ne pourait être poursuivi.

De plus, l'accès aux systèmes informatiques ouverts au public et dont l'utilisation est gratuite ne constituera pas un accès illégal.

B. L'article 3 : L'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 relation avec un système informatique connecté à un autre système informatique. »

Avec cette disposition le secret de communication des données est prévenu.

L'atteinte à la communication des données en pénétrant le système informatique est incriminé par l'intermédiaire de cet article.

L'article 3 sert à la sauvegarde du droit au secret de communication prévu dans l'article 8 de la Convention Européenne sur les droits de l'homme, dans le cas ou ce dernier est attaqué par des voies électroniques telles que le courrier électronique, le transfert de dossier ou le faximile.[244]

Les « moyens techniques » utilisés peuvent être des appareils techniques placés aux voies de communications, les appareils utilisés pour obtenir et/ou enregistrer la communication sans fil, l'utilisation des logiciels de décryptage.

L'expression de « moyen technique » est utilisé afin de limiter l'étendue du champ d'application de cet article.

Ce crime ne peut être commis qu'envers les systèmes informatiques privées, clos au public.

La communication des données informatiques peut être à l'intérieur d'un même système informatique, ou entre deux systèmes informatiques appartenant à une

[244] ibid,p.13.

même personne, ou entre deux systèmes informatiques indépendants en communication, ou entre un système informatique et une personne.

L'accès doit être intentionnelle et illégale. Si la personne accédant au système dispose du droit de le faire, ou si l'accès est accompli pour des raisons de sécurité nationale, nous ne pouvons plus considérer le crime comme illégal.

C. L'article 4 : Atteinte à l'intégrité des données

« 1.Chaque partie adopte les mesures législatives et autres qui se révèlent nécessaire pour ériger en infraction pénale, conformément a 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 sérieux. »

Le but de cette disposition est la prévention des données et des logiciels informatiques contre des actes d'endommagement volontaires (intentionnels) au même titre que les choses ayant une existence matérielle.[245]

L'effacement des données est leur transformation de manière à les rendre méconnaissable ou les rendre intouchable.

Leur altération est la transformation des données informatiques.

Les actes décrits dans l'article 4 de la Convention ne seront punis que s'ils sont commis illégalement.

L'auteur du crime aussi doit avoir agit intentionnellement.

Dans le deuxième paragraphe, il est précisé que les Etats adhérents à la Convention peuvent se préserver le droit d'exiger au cas où les actes cités dans l'article 4 de la Convention aboutissent a des dommages sérieux. Cependant aucune définition du dommage sérieux n'est donnée dans la Convention. Il est laissé aux Etats adhérents d'en définir les limites suivant leur droit national.

Si un Etat adhérant se préserve le droit d'exiger, il devra en expliquer les motifs au Secrétariat Général du Conseil Européen.

---

[245] ibid.p18.

D. L'article 5 : L'atteinte à l'intégrité du système.

« Chaque partie adopte les mesures législatives et autres qui se révèlent nécessaire pour ériger en infraction pénale, conformément a 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 et la suppression des données informatiques »

Le but de cette disposition est l'incrimination au niveau international l'empêchement de l'utilisation légale d'un système informatique et d'autres moyens de télécommunication.

Le droit des administrateurs des systèmes informatiques ou d'autres moyen de télécommunication d'utiliser leur système sans rencontrer d'entraves est préservé ici.

Par « entrave » on entend, l'atteinte au fonctionnement sain d'un système informatique, l'ajout de nouvelles données aux données informatique, l'envoi des données vers d'autres systèmes d'informations, la détérioration des données, l'effacement, la transformation des données informatiques.[246]

L'entrave provoqué doit être grave afin d'être puni.

Il appartient aux Etats de décider à partir de quel moment une entrave pourra être considéré comme grave.

L'entrave doit être illégale et intentionnelle : l'auteur du crime doit avoir agit dans l'intention d'entraver gravement le système informatique.

E. L'article 6 : Abus de dispositifs.

« 1. Chaque partie adopte les mesures législatives et autres qui se révèlent nécessaire 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 a 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 2-5 ci-dessus ;

---

[246] ibid , p.21.

ii. d'un mot de passe, d'un code d'accès ou des données informatiques similaires permettant d'accéder a 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 2-5 ; et

b. La possession d'un élément visé aux paragraphes (a)(1)ou(2) ci-dessus dans l'intention qu'il soit utilisé afin de commettre l'une ou l'autre des infractions visées par l'article 2-5. 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'a pas pour but de commettre une infraction établie conformément de l'article 2 a 5 de la présente Convention, comme en cas d'essais autorisés ou 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 tout autre mise à disposition des éléments mentionnés au paragraphe 1 (a)(2). »

Cette disposition de la convention prévoit en tant que crime indépendant le fait de disposer illégalement les appareils techniques permettant d'accéder aux données informatiques, ou facilitant la commission des délits décrits dans les articles précédents de la convention.

Le législateur Européen veut éviter la formation d'un marché noir pour la vente de ces appareils spécifiques à récolter illégalement des données d'un système informatique. Pour éviter la commission de certains crimes, il incrimine certains actes étant à la source d'autres crimes.[247]

Selon le paragraphe 1(a)1 la procuration, l'importation ou la distribution, dans le but de produire, de vendre ou d'utiliser, d'un appareil technique crée pour commettre les infractions décrites aux articles 2 à 5 de la convention, est défini comme une infraction indépendante.

---

[247] ibid.p.22.

Selon le paragraphe 1(a)2, la procuration, l'importation, la distribution des cryptages informatiques ou des codes d'accès permettant d'accéder illégalement à l'ensemble d'un système informatique ou seulement à l'une de ses parties, en vue de les reproduire, vendre ou utiliser sont considérés comme une infraction indépendante.

L'infraction doit être intentionnelle et illégale. Une intention générale n'est pas suffisante. Une intention particulière prenant en compte la volonté de commettre les infractions décrites dans les articles 2 à 5 de la Convention est requise.

Il est permis aux Etats adhérents de limiter cette infraction lors de sa transposition en Droit interne.

Sous section II : Les infractions informatiques

Les infractions informatiques sont régies par les articles 7 et 8 de la Convention. Ces infractions se rapportent aux crimes traditionnels commis en utilisant un système informatique. La Convention traite la falsification informatique et la fraude informatique comme étant deux types de crimes spéciales de la manipulation des systèmes et des données informatiques.

Ces deux types de crimes ont été pris en compte par la Convention car certaines valeurs juridiques traditionnelles n'étaient pas assez bien protégées par les législations nationales de certains pays, contre les menaces récentes.

A. La Falsification İnformatique

Selon l'article 7 de la Convention ;

« Chaque partie adopte les mesures législatives ou autres qui se révèlent nécessaires pour ériger en infraction pénale contrairement 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 en droit interne une intention frauduleuse ou une intention délictueuse similaire pour que la responsabilité pénale soit engagée. »

L'objectif de cet article est de remplir les vides relatifs au crime traditionnel de falsification, et de créer un nouveau crime parallèle au crime de falsification traditionnelle.

La falsification informatique consiste à tromper autrui en transformant des données informatiques existantes ou en créant de nouvelles données afin de changer leur valeur en tant que preuve dans les opérations juridiques.

La valeur juridique protégée est la sécurité et la crédibilité des données informatiques pouvant être utilisées dans des opérations juridiques.

Cette disposition s'applique à l'équivalent de tous les documents privés ou officiels étant juridiquement valables.[248]

La dernière phrase de la disposition permet aux Etats adhérents, lors de la transposition de cette disposition en droit interne, le droit d'exiger une intention frauduleuse ou délictueuse afin d'engager la responsabilité pénale.

B. La fraude informatique

Selon l'article 8 de la Convention ;

« Chaque partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément a son droit interne, le fait intentionnel et sans droit de causer un préjudice patrimonial a autrui par ;

a. L'introduction, l'altération, l'effacement et la suppression des données informatiques,

b. 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. »

Les principales infractions pouvant être considéré comme fraude informatique sont ;

Les manipulations telles que l'enregistrement ou l'ajout de données fausses, les manipulations sur les logiciels, les interventions au processus d'exploitations des données informatiques.

---

[248] ibid, p.25.

Le but de cet article est de définir en tant que crime, les manipulations et interventions illégales faites au processus d'exploitation des données informatiques afin de transférer illégalement le droit de propriété.

Afin de prendre en compte toutes les manipulations dans le champ d'application, il est utilisé dans le paragraphe (b) une expression générale telle que « toute forme d'atteinte »

Ces manipulations ne peuvent être définies de fraude informatique que si leur but est de réaliser un bénéfice économique illégal provoquant simultanément une perte dans le patrimoine d'autrui.

La manipulation doit être illégale et être à la source d'un bénéfice économique sans droit.

Le crime doit obligatoirement être commis intentionnellement. Une intention générale englobant la réalisation d'un bénéfice économique illégale au détriment de la perte dans le patrimoine d'autrui, est suffisante.

Sous section III : Les infractions de la convention se rapportant au contenu.

Le troisième titre de la Convention relatif aux infractions se rapportant au contenu, est formé d'un seul article : Celui régissant la pornographie enfantine.

Le texte de l'article 9 est comme le suivant :

« Article 9 : İnfractions se rapportant a 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 et la mise a 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 a autrui 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 ci-dessus, la « 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 a 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 (d), et 1(e) et 2(b) et 2(c). »

Dans cet article concernant la pornographie enfantine, le législateur Européen a voulu renforcer les dispositions relatives a la protection du mineur et a élargi le champ d'application du crime portant sur la pornographie enfantine de manière a englober l'utilisation des systèmes informatiques.[249]

Avec cet article, la production électronique de la pornographie enfantine, la possession d'images électroniques portant sur le même sujet et leur distribution sont définis en tant que crime.

Dans le paragraphe 1 (a) de l'article, la production de pornographie enfantine en vue de distribuer à l'aide d'un système informatique est incriminé. Cette disposition fût nécessaire afin de lutter contre ce crime dés la source.

Dans le paragraphe 1 (b), l'offre ou la mise a disposition de la pornographie enfantine par l'intermédiaire d'un système informatique est incriminé. Ici l'offre et la mise à disposition peut être interprété comme une proposition d'image pornographique à autrui ou le recours à quelqu'un afin de procurer ce type d'images. L'objectif de ce paragraphe est en effet d'interdire la formation des liens hypertextes afin de faciliter l'accès aux sites de pornographie enfantine.

Dans le paragraphe 1 (c), la distribution et la diffusion de la pornographie enfantine à travers un système informatique est incriminé.

Par « distribution », on entend la publication du matériel sur Internet.

---

[249] ibid,p.30.

Et la « diffusion » est l'envoi des images de la pornographie enfantine par l'intermédiaire d'un système informatique.

Le fait de « se procurer » ou « procurer a autrui » évoquer dans le paragraphe 1 (d), est l'enregistrement des images de pornographie enfantine de l'Internet au système informatique.

Dans le paragraphe 1 (e), la dissimulation a l'intérieur d'un système informatique ou dans l'un des composants du système (disquette ou disque compact) de la pornographie enfantine est incriminée.

La possession de la pornographie enfantine risque d'activer la demande pour ce type de matériel. Le législateur européen a l'intention d'interdire la pornographie enfantine en incriminant tous les actes allant de la production jusqu'à la possession. En effet l'incrimination de tous ces actes est le moyen de lutte le plus effectif contre l'abus des enfants.

Les critères de la détermination du matériel de la pornographie enfantine sont traités dans le deuxième paragraphe de l'article. Nous pouvons en déduire que dans la détermination de ces critères, la morale publique va devoir être pris en compte.

Cette disposition ne pourra pas s'appliquer aux matériels artistiques, médicales, et scientifiques.

Trois types de matériels, afin de commettre les actes incriminés définis dans le premier paragraphe, sont évoqués dans le deuxième paragraphe de l'article 9. Ce sont ; la représentation d'un mineur se livrant à un comportement sexuel explicite, la représentation d'une personne apparaissant comme un mineur, livré à un comportement sexuel explicite, et la représentation d'images réalistes d'enfant livré dans un comportement sexuel explicite.

Dans le premier cas, la protection directe du mineur des abus sexuels est visée.

Dans les deux autres cas le législateur européen semble vouloir éviter la formation d'un sous culture portant sur l'abus des enfants.

Dans le troisième paragraphe, une définition du mineur est donnée : « toute personne âgée de moins de 18 ans ». Cette définition est en concordance avec celle donnée dans la Convention des Nations Unis portant sur les Droits d'Enfants. L'âge en question ici est celle qui est relative à l'age minimum qu'une

personne devrait avoir pour servir d'objet sexuel dans la production de matériel pornographique. Il ne s'agit pas ici de l'âge minimum à laquelle une personne peut s'engager de manière légale dans une activité sexuelle.

Il est permis cependant aux Etats adhérant de fixer cette limite d'âge à 16 en transposant cette disposition dans leur droit interne.

Cette infraction ne peut être réalisée qu'intentionnellement. La responsabilité pénale d'une personne ne portant pas l'intention de produire, de diffuser ou de distribuer du matériel de la pornographie enfantine, ne pourra pas être engagée.

Le quatrième paragraphe reconnaît aux Etats adhérents le droit de porter des réserves à l'application des alinéas (d) et (e) du premier paragraphe, et des alinéas (b) et (c) du deuxième paragraphe. Cependant ces réserves doivent être signalés au secrétariat général du Conseil de l'Europe lors de la signature de la Convention.

Sous section IV : Les infractions liées aux atteintes à la propriété intellectuelles et aux droits connexes.

Ces infractions sont prises en compte par l'article 10 de la Convention dont le texte est comme le suivant :

« Article 10 : les infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes.

1. Chaque partie adopte les mesures législatives et autres qui se révèlent nécessaire pour ériger, en infraction pénale, conformément à son droit interne, les atteintes à la propriété intellectuelle définie par la législation de ladite Partie, conformément aux obligations que celle-ci a souscrites en application de la Convention universelle sur le droit d'auteur révisée à Paris le 24 juillet 1971, de la Convention de Berne pour la protection des œuvres littéraires et artistiques, de l'accord sur les aspects commerciaux de la propriété intellectuelle et Traité de l'OMPİ définie par la législation de ladite sur la Propriété İntellectuelle, à l'exception de tout droit moral conféré par ces Conventions, lorsque de telle 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 nécessaire pour ériger en infraction pénale, conformément à son droit interne, les atteintes aux droits connexes définis par la législation de la dite Partie conformément aux obligations que celle-ci a souscrites en application de la Convention internationale sur la protection des artistes interprètes ou exécutant des producteurs de phonogrammes et des organismes de radiodiffusion faite a Rome (Convention de Rome), de l'accord sur les aspects commerciaux des droits de propriété intellectuelle et du traité de l'OMPİ sur les interprétations, exécution et phonogramme, a 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.

3. Une partie peut, dans des circonstances bien délimitées, se réserver le droit de ne pas imposer de responsabilité pénale au titre des paragraphes 1 et 2 du présent article, à condition que d'autres recours efficace soient disponibles et qu'une telle réserve ne porte pas atteinte aux obligations internationales incombant à cette partie en application des instruments mentionnés aux paragraphes 1et 2 du présent article. »

L'article fait des renvois aux conventions internationales conclues jusqu'à ce jour et incrimine la violation des dispositions de ces Conventions par l'intermédiaire des systèmes informatiques.

Section III : Droit de procédure pénale

Les Etats adhérents à la Convention Européenne contre la Cybercriminalité sont tenus d'harmoniser aussi leur droit de procédure pénale suivant les dispositions de la Convention.

En effet, les preuves se trouvant que dans le milieu électronique risquent d'être facilement et rapidement (dans quelques secondes) détruites. C'est la raison pour laquelle les mesures préventives adaptées à ces caractéristiques du milieu électronique doivent être élaborées.[250]

Les dispositions relatives à la procédure pénale sont prévues entre les articles 14 à 22 de la Convention.

---

[250] Keskin Serap, "Avrupa Konseyi Siber Suç Sözleşmesinde Ceza Muhakemesine ilişkin Hükümlerin Değerlendirilmesi", İÜHFM, Cilt LIX, sene 2001, cilt : 1-2, p. 155.

Les mesures préventives prévues dans la Convention, sont une forme particulière, de la perquisition et de la réquisition.

Dans la Convention, des mesures préventives préalables à la perquisition et à la réquisition, sont prévues en raison du caractère aléatoire du milieu électronique : en effet, il est parfois obligé de préserver certaines données informatiques même avant la mise en œuvre des mesures préventives, car celles-ci risquent de disparaître très rapidement dans le cas où ils peuvent servir de preuve a un crime.

Ces mesures préventives préalables sont régies dans la deuxième section de la Convention, ce sont ;

La conservation rapide des données informatiques stockées (art.16), la conservation et la divulgation rapides de données relatives au trafic (art.17), l'injonction de produire (art.18), la perquisition et la saisie des données stockées (art.19), le collecte en temps réel des données relatives au trafic (art.20) et enfin l'interception de données relatives au contenu (art.21).

On ne peut avoir recours à ces mesures préventives qu'en la présence d'une investigation pénale. Car la décision de recours à ces mesures risquent de porter atteinte au secret de la vie privée, ainsi qu'à la liberté de communication.

C'est pour cette raison que ces mesures devront être mise en œuvre que dans le cas de(s) crime(s) et d'auteur(s) de crimes concrets.

Sous section I : Le principe de respect aux droits et libertés de l'homme et le principe de proportionnalité dans l'application des mesures préventives informatiques.

Les conditions et les sauvegardes sont précisées dans l'article 15 de la Convention.

Les Etats adhérents sont tenus de préserver et de respecter les droits et libertés de l'homme en transposant les dispositions de cette convention dans leur droit interne. Ils sont surtout tenus d'instaurer un équilibre entre les mesures préventives et l'acte poursuivi. Les éléments pouvant instaurer cet équilibre ne sont pas précisés dans la Convention. Il est laissé à la libre appréciation des Etats d'en décider. Mais la Convention précise que les standards minimums communs créent par les autres conventions Internationales doivent être pris en compte. Ces

Conventions sont la Convention de Sauvegarde des Droits de l'Homme et des libertés fondamentales de 1950 ainsi que ses protocoles annexes, le Pacte international relatif aux droits civils et politiques des Nations Unis de 1966 et les autres actes internationaux signés au niveau des régions.[251]

D'autre part le principe de proportionnalité devra être respecté dans la mise en œuvre des mesures préventives : il doit avoir un équilibre entre le crime et la mesure préventive. Il ne faut utiliser une mesure préventive pouvant entraîner des résultats sérieux pour des délits mineurs. De même, il ne faut pas engager des mesures légères pour des crimes graves.

La Convention prévoit l'instauration d'un mécanisme indépendant de contrôle pour surveiller si les conditions de recours aux mesures préventives sont remplies.

Le respect du droit de ne pas s'inculper ou de ne pas inculper ses proches afin de prouver un crime est reconnu. De même, le droit des personnes qui en droit général, peuvent s'abstenir d'apporter témoignage à un crime, est épargné ici aussi.

Les Etats adhérents à la Convention devront prendre en compte l'intérêt public, et la bonne administration de la justice.

Sous section II : Les Mesures préventives informatiques prévues dans la convention.

A. La Conservation rapide des données informatiques stockées

" Article 16 – Conservation rapide de données informatiques stockées

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour permettre à ses autorités compétentes d'ordonner ou d'imposer d'une autre manière la conservation rapide de données électroniques spécifiées, y compris des données relatives au trafic, stockées au moyen d'un système informatique, notamment lorsqu'il y a des raisons de penser que celles-ci sont particulièrement susceptibles de perte ou de modification.

2. Lorsqu'une Partie fait application du paragraphe 1 ci-dessus, au moyen d'une injonction ordonnant à une personne de conserver des données stockées

[251] ibid,p.160.

spécifiées se trouvant en sa possession ou sous son contrôle, cette Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger cette personne à conserver et protéger l'intégrité desdits données pendant une durée aussi longue que nécessaire, jusqu'à maximum 90 jours, afin de permettre aux autorités compétentes d'obtenir leur divulgation. Une Partie peut prévoir qu'une telle injonction soit renouvelée par la suite.

3. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger le gardien des données ou une autre personne chargée de conserver celles-ci à garder le secret sur la mise en œuvre desdites procédures pendant la durée prévue par son droit interne.

4. Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15."

C'est une mesure préventive prévue afin de pouvoir réaliser dans le futur, la perquisition ou la réquisition. Le but de cette disposition est la conservation des données informatiques d'une manière intacte, c'est-à-dire sans être effacé ou transformé.[252]

Les sujets de cette mesure préventive sont les données ramassées et stockées par les fournisseurs d'accès et les collecteurs de données informatiques.

La Convention ainsi impose au FAİ le devoir de stocker des informations à propos personnes ou des institutions bénéficiant de son service.

Cette mesure ne peut être mis en œuvre que lors d'une investigation pénale concrète : L'acte et l'auteur de l'acte doivent être tous les deux déterminés. D'autre part, il faudrait préciser quelle(s) donnée(s) doit être protégée.

On ne peut avoir recours à cette mesure préventive, que dans le cas la préservation des données en question est douteuse.

La personne sur qui cette mesure préventive va devoir s'appliquer est celle qui dispose de ces informations stockées. Le devoir de protection des données de cette personne ne peut pas être plus de 90 jours. Cependant la durée doit être assez longues pour prendre les autres mesures préventives telle que la perquisition et la réquisition.

---

[252] ibid.p.161.

La convention prévoit aussi pour celui qui est tenu de protéger les données informatiques, le devoir de garder le secret sur la mise en œuvre de ces procédures. Ce devoir aussi est limité par une durée dont la longueur devra être décidée par les Lois nationales.

B. La Conservation et divulgation rapides de données relatives au trafic

"Article 17 – Conservation et divulgation rapides de données relatives au trafic

1. Afin d'assurer la conservation des données relatives au trafic en application de l'article 16, chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour:

a. veiller à la conservation rapide de ces données relatives au trafic, qu'un seul ou plusieurs fournisseurs de service aient participé à la transmission de cette communication; et

b. assurer la divulgation rapide à l'autorité compétente de la Partie, ou à une personne désignée par cette autorité, d'une quantité de données relatives au trafic suffisante pour permettre l'identification des fournisseurs de service et de la voie par laquelle la communication a été transmise.

2. Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15."

Cet article apporte des obligations concrètes.

Les données relatives au trafic sont définis dans l'article 1/d. de la Convention.

Selon cette définition, l'expression « données relatives au trafic » désigne « toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type du service sous-jacent. »

L'origine d'une donnée relative au trafic, peut être un numéro de téléphone, une adresse IP pouvant qualifier l'outil de communication par lequel, le fournisseur de service accomplit ses fonctions.[253]

La destination est les informations relatives à l'outil de communication vers lequel les données sont envoyées.

Le type de service sous jacent est le type de service utilisé a l'interieur du réseau : transfert de dossier, courrier électronique, courrier instantané (etc.) ...

Le 17.ème article vise la protection des données relatives au trafic entre tous les fournisseurs de service participant à l'itinéraire d'une information.

Par la protection, on entend la continuation de la préservation des données informatiques déjà stockées. La décision des moyens de protection est laissée aux législations nationales.

Le 17.eme article prévoit encore une obligation au fournisseur de service, d'assurer la divulgation rapide a l'autorité compétente une quantité de données relatives au trafic suffisantes pour permettre l'identification des fournisseurs de service et de la voie par laquelle la communication a été transmise.

Les autorités compétentes sont tenues de préciser le type de données relatives au trafic à divulguer.

Par l'intermédiaire de cette disposition les autorités compétentes vont pouvoir décider de la nécessité d'étendre la mesure préventive à d'autres fournisseurs de service.

C . L' Injonction de produire.

"Article 18 – Injonction de produire

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner :

a. à une personne présente sur son territoire de communiquer les données informatiques spécifiées, en la possession ou sous le contrôle de cette personne, et stockées dans un système informatique ou un support de stockage informatique; et

[253] ibid,p. 165.

b. à un fournisseur de services offrant des prestations sur le territoire de la Partie, de communiquer les données en sa possession ou sous son contrôle relatives aux abonnés et concernant de tels services;

2. Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

3. Aux fins du présent article, l'expression « données relatives aux abonnés » désigne toute information, contenue sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de service et qui se rapporte aux abonnés de ses services, autres que des données relatives au trafic ou au contenu, et permettant d'établir:

a. le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service ;

b. l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de service ;

c. toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de service."

Par l'intermédiaire de cet article, les autorités d'investigation pénale vont pouvoir demander à une personne se trouvant sur leur territoire nationale, de leur fournir les données informatiques qui sont sous sa contrôle ou dans sa propriété, et aux fournisseurs de services de donner les informations se rapportant aux abonnés de leurs services.

Les sujets de l'injonction de produire sont les données stockées.

Cette mesure préventive ne peut s'appliquer que dans la mesure où la personne privée et les fournisseurs de service stockent les données en question. Sinon la mesure n'aura plus de valeur.

La Convention a laissé aux Etats adhérents la possibilité de décider de différentes conditions, de différentes autorités et procédures en fonction des données

qu'il cherche à obtenir. Cependant l'Etat adhérant doit respecter le principe de proportionnalité de la mesure. Le principe de secret est laissé au choix des législations nationales.

La production des données relatives au trafic, peut se faire par courrier électronique (on-line), en enregistrant sur une disquette, en imprimant les données sur une feuille (etc.)... l'Etat adhérant va devoir préciser le moyen de production avec l'injonction.

Dans l'article 18 est défini enfin l'expression de « données relatives aux abonnés ». Ce sont les informations retenues par les fournisseurs de service et se rapportant a l'abonné : l'identité e celui-ci, l'adresse de son domicile, son numéro de téléphone, le contrat de service, les factures, les informations sur les moyens de paiement, le type de service de communication utilisé, la durée du service procuré et ainsi de suite.

Enfin, l'injonction de produire ne pourrait être décidé que dans le cadre d'une investigation pénale concrète.

D. La Perquisition et la saisie de données informatiques stockées

"Article 19 – Perquisition et saisie de données informatiques stockées

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à perquisitionner ou à accéder d'une façon similaire :

a. à un système informatique ou à une partie de celui-ci ainsi qu'aux données informatiques qui y sont stockées ; et

b. à un support du stockage informatique permettant de stocker des données informatiques

Sur son territoire.

2. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour veiller à ce que, lorsque ses autorités perquisitionnent ou accèdent d'une façon similaire à un système informatique spécifique ou à une partie de celui-ci, conformément au paragraphe 1 (a), et ont des raisons de penser que les données

recherchées sont stockées dans un autre système informatique ou dans une partie de celui-ci situé sur son territoire, et que ces données sont légalement accessibles à partir du système initial ou disponibles pour ce système initial, lesdites autorités soient en mesure d'étendre rapidement la perquisition ou un d'un accès d'une façon similaire à l'autre système.

3. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à saisir ou à obtenir d'une façon similaire les données informatiques pour lesquelles l'accès a été réalisé en application des paragraphes 1 ou 2. Ces mesures incluent les prérogatives suivantes :

a. saisir ou obtenir d'une façon similaire un système informatique ou une partie de celui-ci ou un support de stockage informatique ;

b. réaliser et conserver une copie de ces données informatiques ;

c. préserver l'intégrité des données informatiques stockées pertinentes ; et

d. rendre inaccessibles ou enlever ces données informatiques du système informatique consulté.

4. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner à toute personne connaissant le fonctionnement du système informatique ou les mesures appliquées pour protéger les données informatiques qu'il contient de fournir toutes les informations raisonnablement nécessaires, pour permettre l'application des mesures visées par les paragraphes 1 et 2.

5. Les pouvoirs et procédures mentionnés dans cet article doivent être soumis aux articles 14 et 15."

Cette mesure ne peut être mise en œuvre que dans le cadre d'une investigation pénale concrète.

Il s'agit de la perquisition et de la réquisition des données informatiques stockées en vue d'obtenir des preuves.

Ces mesures sont la forme particulière de la perquisition et de la réquisition dans le monde informatique.[254]

Selon cet article, un système informatique ou sa partie détachable ou les données qui y sont enregistrées vont pouvoir devenir les sujets de ces mesures.

Ces mesures ne peuvent être appliquées qu'aux données déjà stockées.

La collecte (ou réquisition) comprend la mainmise sur le support dans lequel les données informatiques y sont enregistrées et la reproduction de ces données sur d'autres supports. Elle comprend également l'utilisation des logiciels nécessaires pour accéder aux données en question.

La collecte signifie tout simplement la détention du contrôle des données informatiques.

Le 19.eme article prévoit également, afin de préserver la qualité de preuve des données, de les rendre inaccessible, de les déplacer et même de les effacer.

Le dernier paragraphe prévoit l'aide de personnes dotées de formations techniques aux autorités judiciaires, dans l'application de ces mesures.

Cependant ce devoir d'aide doit être tenu dans des limites raisonnables.

La convention laisse à la libre appréciation des Etats le fait de tenir ou non l'application de ces mesures secrète.

E.La Collecte en temps réel des données relatives au trafic.

"Article 20 – Collecte en temps réel des données relatives au trafic

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à :

a. collecter ou enregistrer par l'application de moyens techniques existant sur son territoire ;

b. obliger un fournisseur de services, dans le cadre de ses capacités techniques existantes, à :

i. collecter ou enregistrer par l'application de moyens techniques existant sur son territoire, ou

---

[254] ibid,p.172.

ii. prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer,

En temps réel, les données relatives au trafic associées à des communications spécifiques transmises sur son territoire au moyen d'un système informatique.

2. Lorsqu'une Partie, en raison des principes établis de son ordre juridique interne, ne peut adopter les mesures énoncées au paragraphe 1(a), elle peut à la place, adopter les mesures législatives et autres qui se révèlent nécessaires pour assurer la collecte ou l'enregistrement en temps réel des données relatives au trafic associées à des communications spécifiques transmises sur son territoire par l'application de moyens techniques existant sur ce territoire.

3. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger un fournisseur de services à garder secrets le fait que l'un quelconque des pouvoirs prévus dans le présent article a été exécuté, ainsi que toute information à ce sujet.

4. Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15."

La collecte en temps réel des données a été considérée comme une sérieuse atteinte à la liberté de communication. Effectivement, cette mesure de prévention s'applique au moment où les données informatiques circulent dans le réseau.

Elle peut se réaliser par la reproduction spontanée des données informatiques en pleine circulation.

Pendant la collecte en temps réel des données relative, la circulation des données informatique n'est pas empêchée, celle-ci arrive sans problème à leur destination.

La collecte de tout types de données (privées ou publiques) va pouvoir être décidé.

Selon la Convention, cette mesure pourra s'appliquer à tout type de crime. Mais les Etats adhérents dispose du droit de limiter son application qu'à certains types de crime.

L'objectif de cette mesure est de collecter les preuves des accès illégaux aux systèmes informatiques, de la transmission des virus, des crimes relatives à la pornographie enfantine.

Cette mesure ne pourra s'appliquer que dans le cadre d'une investigation pénale concrète. Il faut cependant que l'une des parties a la communication, ou l'un des appareils à travers lequel les données circulent se trouvent dans le territoire national.

Il faudra que l'autorité compétente précise dans sa décision les informations sur lesquelles la mesure devra porter.

Cependant les personnes dotées d'une connaissance technique sont tenues d'aider les autorités judiciaires compétentes dans l'investigation du crime. Ces personnes peuvent selon le cas collecter eux-mêmes les données servant de preuve.

La Convention prévoit que cette collecte soit faite en secret. Les personnes auxiliaires peuvent être obligé à tenir le secret.

F. L'Interception de données relatives au contenu

Article 21 – Interception de données relatives au contenu

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes relativement à un éventail d'infractions graves à définir en droit interne, à :

a. collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire ; et

b. obliger un fournisseur de services, dans le cadre de ses capacités techniques existantes, à :

i. collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire, ou

ii. prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer,

En temps réel, les données relatives au contenu de communications spécifiques sur son territoire, transmises au moyen d'un système informatique.

2. Lorsqu'une Partie, en raison des principes établis de son ordre juridique interne, ne peut adopter les mesures énoncées au paragraphe 1(a), elle peut à la place adopter les mesures législatives et autres qui se révèlent nécessaires pour assurer la collecte ou l'enregistrement en temps réel des données relatives au contenu de communications spécifiques transmises sur son territoire par l'application de moyens techniques existant sur ce territoire.

3. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger un fournisseur de services à garder secrets le fait que l'un quelconque des pouvoirs prévus dans le présent article a été exécuté, ainsi que toute information à ce sujet.

4. Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et15.

Il n'y a pas de définition portant sur les données relatives au contenu dans la Convention.

Les données relatives au contenu sont tous les données qui ne sont pas relatives au trafic : elles peuvent porter sur le contenu de la communication ou la signification ou l'intention qu'elle contient.

L'interception de données relatives au contenu est le fait de rejoindre spontanément au contenu de la communication.

C'est la mesure qui porte le plus lourdement atteinte au secret de la vie privée et a la liberté de communication.

Avec cette mesure, l'itinéraire du message n'est pas entravé : le message parvient a sa destination sans rencontrer d'obstacle.

Cette mesure implique la reproduction d'une copie des informations en copie.

Il n'est pas fait de différence entre les informations privées ou publiques dans l'application de l'interception.

Comme cette mesure porte des grandes atteintes aux libertés fondamentales, la Convention prévoit son application que pour les crimes graves.

La Convention prévoit que les Etats adhérents devront prendre en compte les dispositions de la Convention Européenne des Droits de l'Homme et les décisions

de La Cour Européenne des Droits de l'homme, dans la transposition de cette mesure préventive dans son droit interne.

Cette mesure peut être un outil important d'investigation, notamment pour les crimes tels que la dénonciation calomnieuse, l'injure, la pornographie enfantine, la contrebande de drogue.

Afin d'intercepter les données relatives au contenu, les Etats doivent construire une infrastructure et coopérer avec les fournisseurs de service. Le devoir de garder le secret est aussi valable pour l'application de cette mesure.

G. Les dispositions relatives a la compétence.

"Article 22 – Compétence

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour établir sa compétence à l'égard de toute infraction pénale établie conformément aux Articles 2 – 11 de la présente Convention, lorsque l'infraction est commise:

a. sur son territoire ;

b. à bord d'un navire battant pavillon de cette Partie ;

c. à bord d'un aéronef immatriculé dans cette Partie ;

d. par un de ses ressortissants, si l'infraction est punissable pénalement là où elle a été commise ou si l'infraction ne relève de la compétence territoriale d'aucun Etat.

2. Chaque Partie peut se réserver le droit de ne pas appliquer, ou de n'appliquer que dans des cas ou conditions spécifiques, les règles de compétence définies aux paragraphes 1b – 1d du présent article ou dans une partie quelconque de ces paragraphes.

3. Chaque Partie adopte les mesures qui se révèlent nécessaires pour établir sa compétence à l'égard de toute infraction mentionnée à l'article 24, paragraphe 1 de la présente Convention, lorsque l'auteur présumé de l'infraction est

présent sur son territoire et ne peut être extradé vers une autre Partie au seul titre de sa nationalité, après une demande d'extradition.

4. La présente Convention n'exclut aucune compétence pénale exercée par une Partie conformément à son droit interne.

5. Lorsque plusieurs Parties revendiquent une compétence à l'égard d'une infraction présumée visée dans la présente Convention, les Parties concernées se concertent, lorsque cela est opportun, afin de décider quelle est celle qui est la mieux à même d'exercer les poursuites."

L'article 22 est la dernière disposition de la Convention concernant le droit de la procédure pénale.

La convention énumère ici les critères à adopter pour décider le tribunal compétent au jugement des crimes énumérés entre les articles 2 a 11.

Les principes énumérés sont les suivants :

- Le principe de territorialité : l'Etat national est tenu de juger les crimes commis sur son territoire. (En Droit Turc, la situation est ainsi pour tous les crimes.)

Si la personne attaquant le système informatique, ou le système victime de l'attaque se trouve dans le territoire de l'Etat, ce dernier va être compétent pour le jugement du crime.

- le principe de personnalité selon l'auteur du crime : selon ce principe, un Etat va pouvoir être doté de la compétence de juger son citoyen ayant commis un acte criminel dans le territoire d'un Etat étranger, à condition que cet acte soit aussi incriminé par la législation de l'Etat étranger.

De même selon ce même principe, l'Etat va pouvoir juger l'acte criminel de son citoyen qui échappe à la compétence de jugement des Etats sur le territoire desquels le crime a été commis.

La convention prévoit pour les Etats adhérents la possibilité de réserver leur compétence de jugement suivant certaines conditions. Mais un Etat adhérant ne dispose pas du droit de ne pas juger son citoyen, dont il a refusé son extradition, pour avoir commis un crime dans le territoire d'un autre Etat.

La convention propose, pour la situation dans laquelle les complices d'un crime commis en complicité se trouvent dans des pays différentiels, d'attribuer la compétence de jugement au pays qui est le mieux placé pour assurer cette fonction.

CONCLUSİON

Les caractéristiques de la criminalité sur Internet peuvent être résumés de la manière suivante :

Les crimes commis sur İnternet sont de deux types ;

Dans la première catégorie, les crimes s'apparentent aux crimes conventionnels du monde réel. En effet, il semble que ces crimes ont trouvé dans l'Internet un nouveau milieu pour s'épanouir. C'est le cas notamment pour l'escroquerie, la falsification, la pornographie enfantine, les atteintes à la vie privée, les atteintes aux droits d'auteur et aux droits des marques (...). Dans tous ces cas précités, l'Internet sert de simple support à la réalisation du crime. Les valeurs juridiques violées sont les mêmes, l'auteur du crime agit avec la même intention et motifs criminels, enfin, les résultats des crimes sont les mêmes.

La deuxième catégorie est formée par l'ensemble des crimes spécifiques à Internet. C'est le cas de l'accès frauduleux dans un système informatique, la détérioration des données informatiques (...). İl ne s'agit plus des crimes traditionnels, ici les systèmes informatiques formant le réseau Internet ne sont plus les supports des crimes, mais ils en deviennent les cibles.

Ces deux catégories forment ensemble ce qu'on appelle « les cybercrimes ».

Ces cybercrimes requièrent une forme spéciale d'investigation et de répression en raison de leur caractère international. En effet, l'Internet étant une innovation abolissante, toute sorte de frontières nationales, les résultats des crimes commis sur Internet se répercutent en général en dehors des frontières des pays dans lequel ils sont commis.

Dés lors il faut instaurer une régulation à trois niveaux :

Premièrement au niveau des sujets de l'İnternet, une forme d'autorégulation voire même de corégulation semble nécessaire pour la répression des délits mineurs. Deuxièmement au niveau étatique : il n'est presque jamais de possible de poursuivre, les auteurs de crimes sur Internet. Ils sont en général introuvables et/ou insolvable. A ce point les institutions étatiques doivent dans un premier temps, adopter une politique qui vise essentiellement la prévention de ces crimes. Elles doivent instaurer un régime de responsabilité pénale pour les sujets de l'Internet. Cependant, il faut être vigilant car la simple transposition des principes du

droit de la presse ne semble pas être suffisante en raison des différents caractères de ces deux types d'activité d'édition. Les Etats doivent prévoir dans un deuxième temps de nouvelles mesures préventives dans la collecte des preuves sur Internet : le monde virtuel étant un milieu dans lequel ou tout circule/se déroule avec une extrême rapidité, il n'est plus possible de mener des investigations en se servant des mesures préventives classiques. Il faut que l'Etat prévoie dans sa législation nationale des « armes de guerre » appropriés. Cependant, il doit veiller de ne pas porter atteinte à la liberté d'expression et de communication, les « raisons d'être » de l'Internet. Enfin troisièmement, une coopération internationale est nécessaire. Les Etats doivent s'entraider dans la poursuite et le jugement des cybercrimes.

En ce qui concerne, le cas de la Turquie ; les propos selon lesquelles la Turquie ne poursuit pas correctement les avancées technologiques et qu'il existe un vide juridique dans la répression des crimes commis sur İnternet est un mythe. La répression des crimes conventionnels commis sur İnternet ne pose pas de problèmes dans la mesure où les supports du crime ne sont pas énumérés d'une manière exhaustive dans le texte de l'article. Pour les crimes dont la cible est les systèmes informatiques formant le réseau İnternet, les amendements accomplis en 1991 dans le code pénal turc semblent régler l'affaire en grande partie.

Cependant, le Nouveau Code Pénal Turc est loin de fournir un arsenal répressif complet pour les crimes d'İnternet et présente des lacunes. Dans un premier temps, elle ne donne aucune définition des notions telle que « données » et « système informatique ». Cela risque d'entraîner des confusions dans la pratique. Bien que la Convention Européenne sur la Cybercriminalité ait prévue un crime de falsification informatique comme un crime à part entier, le nouveau code pénal n'en prévoit pas un. Hors de nos jours, la plupart des documents juridiques sont crées à l'aide des systèmes informatiques. Les personnes commettant ce crime vont être punies au même titre que ceux ayant commis le délit de falsification conventionnel. D'autre part, l'accès frauduleux au système informatique est prévu dans le nouveau code, mais la possession et la vente des outils de décryptage servant à la réalisation de ce crime ne sont pas incriminées. Hors pour une lutte sincère contre ce crime, il aurait fallu incriminer cet acte qui est la source de l'autre crime.

D'ailleurs la Convention Européenne sur la Cybercriminalité incrimine, la possession et la commercialisation des outils de décryptage facilitant l'accès frauduleux dans le système informatique.

Finalement nous pensons que l'adhésion de la Turquie à la Convention Européenne sur la Cybercriminalité et la promulgation d'une Loi propre à l'İnternet sont indispensables.

Bibliographie

A) Les Ouvrages Généraux

Dönmezer Sulhi – Erman Sahir, Nazari ve Tatbiki Ceza Hukuku, Cilt I, 12.Bası, İstanbul, Beta Yayınevi, 1997

Dönmezer Sulhi – Erman Sahir, Nazari ve Tatbiki Ceza Hukuku, Cilt III, 12.Bası, İstanbul, Beta Yayınevi, 1997

İçel Kayıhan, Kitle Haberleşme Hukuku, İstanbul, Yenilenmiş beşinci Bası, Beta Yayınevi, 2001

İnan Aslan, İnternet El Kitabı, 9.Bası, İstanbul, Sistem Yayıncılık, 2001

Kalbag Asha, Dünyayı Saran Ağ : www , 5.Bası, Ankara, Tübitak Yayınları, 2000

Kalbag Asha, Bilgisayar'daki Adresiniz Web Sitesi, 5.Bası, Ankara, Tübitak Yayınları, 2000

Özek Çetin, Türk Basın Hukuku, İstanbul,1978,.

Sarıhan Tan Deniz , Herkes için İnternet, İstanbul, Desnet Yayınları, 1998

Tekinalp Ünal , Fikri Mülkiyet Hukuku, 2.Bası, İstanbul, Beta Yayınevi, 2002

B) Les Ouvrages Spécialisés

Akdeniz Yaman – Walker Clive – Wall David , The İnternet Law and Society, United Kingdom - Essex, Longman Pearson Education, 2000

Akdeniz Yaman, Sex on the Net : The Dilemna of Policing Cybersapce, United Kingdom – Reading, South Street Press; 1999

Châtelain Yannick –Roche Loick , Hackers ! Cinquieme Pouvoir , Paris, Maxima Laurent Du Mesnil-Editeur, 2002

Himanen Pekka, L'Ethique Hacker et l'Esprit de l'Ere de l'İnformation , Paris, Exils Editeur , 2001

Jenkins Philip, Beyond Tolerance : Child Pornography on The Net, New York, University Press , 2001

Özdilek Osman, İnternet ve Hukuk, İstanbul, Papatya Yayıncılık, 2002

Pansier Fréderic Jerôme – Jez Emmanuel, La Criminalité sur İnternet, Paris , Que Sais Je ? Puf, 2001

Sınar Hasan, İnternet ve Ceza Hukuku, İstanbul, Beta Yayınevi, 2001

Sırabaşı Volkan , İnternet ve Radyo Televizyon Aracılığıyla Kişilik Haklarına Tecavüz (İnternet Rejimi), Ankara, Adalet Yayınevi, 2003

Yazıcıoğlu Yılmaz, Kriminolojik Sosyolojik ve Hukuki boyutları ile Bilgisayar Suçları, İstanbul, Alfa Basım Yayım Dağıtım, 1997

Yenidünya A.Caner, Değirmenci Olgun, Bilişim Suçları, İstanbul, Legal Yayıncılık San. Ve Tic.Ltd.Şti, 2003

C) Thèses Et Mémoires

Jougleux Philippe, La Criminalité dans le Cyberespace, Université de Droit d'Economie et des Sciences D'Aix Marseille, Faculté de Droit et de Science Politique d'Aix Marseille, Mémoire de D.E.A, Droit des Médias, Année de Soutenance 1999.

De Marco Estelle, Le Droit Pénal Applicable sur İnternet, Université de Montpellier 1, İnstitut de Recherche et d'Etudes pour le Traitement de l'İnformation Juridique, Mémoire de D.E.A. İnformatique et Droit, Annee de soutenance 1998 . d'après http ://www.juriscom.net (11.10.2003)

Lavanchy Morgan, La Responsabilité Délictuelle sur Internet en droit suisse, Université de Neuchâtel – Faculté de droit,Thèse de licence, Session 2002, d'après http : // www.droit-technologie.org (21.01.2005)

D) Périodiques

a) Les revues spécialisées

İstanbul Üniversitesi Hukuk Fakültesi Mecmuası Cilt : LIX Sayı : 1-2 Sene :2001

Dokuz Eylül Üniversitesi 21-22 Mayıs Uluslararası İnternet Hukuku Sempozyumu, İzmir, Dokuz Eylül Üniversitesi Yayınları, 2002

b) Les articles

Erman Barış, Alman Hukukunda İnternetten kaynaklanan ceza sorumluluğu, İÜHFM, Cilt LIX, sene 2001, cilt : 1-2, p. 224

İçel, Kayıhan "Avrupa Konseyi Siber Suç Politikasının Ana İlkeleri" İÜHFM, Cilt LIX, sene 2001, cilt : 1-2, p.3

Kangal Zeynep T. "Fransa internet yoluyla işlenen suçlardan doğan ceza sorumluluğu"
İÜHFM, Cilt LIX, sene 2001, cilt : 1-2, p. 228

Keskin Serap, "Avrupa Konseyi Siber Suç Sözleşmesinde Ceza Muhakemesine ilişkin Hükümlerin Değerlendirilmesi", İÜHFM, Cilt LIX, sene 2001, cilt : 1-2, p. 155

Sokullu Akıncı Füsun, "Avrupa Konseyi Siber Suç Sözleşmesinde Yer Alan Maddi Ceza Hukukuna ilişkin Düzenlemeler ve özellikle Çocuk Pornografisi" İÜHFM Cilt LIX; Sene 2001, sayı 1-2 , p.11

Tezcan, Durmuş "İnternet karşısında özel hayatın korunması"
Dokuz Eylül Üniversitesi 21-22 Mayıs Uluslararası İnternet Hukuku Sempozyumu, İzmir, Dokuz Eylül Üniversitesi Yayınları, 2002, p.531

c) Les articles juridiques sur İnternet

Balassoupramaniane İndragandhi, "La pornographie enfantine, la réponse du Conseil d'Europe" d'après
www.barreau.qc.ca/journal/frameset.asp?article=/journal/vol35/no 4/droitcompare.(17.08.2004)

Bitoun, Jacques Georges « De la protection de la vie privée : des cookies indigestes », http://securinet.free.fr./annexe/cookiesindigestes.html (01.09.2004)

Brenner, Susan W, « İs there such a Thing as Virtuel Crime ? » http://boalt.org/CCLR/v4/v4brenner.htm (06.12.2003)

Byars Will-Sproles Jimmy "Examples of Cyber-terrorism"
www.cs.etsu.edu/gotterbarn/stdntppr/cases/htm (22.12.2003)

Dibbel Julian, " A Rape in Cyberspace" (or Tiny Society And How to Make one), www.levity.com/julian/bungle (06.12.2003)

Dufresne, Jacques « Histoire d'Internet » http://agora.qc.ca/rech_int.html (27.05.2004)

Hayward, Douglas « Net-Based Terrorism A Myth »
www.techweb.com/wire/news/1997/11/1119terrorism.html (23.12.2002)

Karaoğlu,Erol « Bir web sitesine diğer bir web sitesinden bağlanma (=linking) ve doğurduğu hukuksal sorunlar »
www.hukukcu.com/bilimsel/kitaplar/linking.htm (06.10.2003)

Özdilek, Ali Osman « Film Korsanlığı ve İnternet »
www.hukukcu.com/bilimsel/kitaplar (06.10.2003)

Raghavan Tara Myrthri "İn fear of Cyberterrorism: An Analysis of the Congressional response"
http://www.jltp.uiuc.edu/recdev/articles/Raghavan/Raghavan.htm (21.05.2004)

Verbiest, Thibault « Quelle responsabilité pour les acteurs de l'İnternet ? La diffusion des informations sur le réseau peut elle engager la responsabilité des

partenaires techniques ? », www.juriscom.net/pro/1/resp19990121.htm (09.12.2003)

Vermeys, Nicolas, "L'union fait la force pour Napster" www.juriscom.net.actu.achv./200011.htm (05.05.2004)

d) Les Sites İnternet divers

« Alerte a l'escroquerie » www.indexel.net/1_20_2931_/alerte_a_l'_escroquerie.htm (02.09.2004)

« Backgrounds &Trends / "İnternet Background", Road and Crossroads of İnternet History » www.netvalley.com/index.html (04.12.2003)

« La Cyberpédophilie en Droit Comparé » http:/users.swing.be/criminologie/contenus/ch3/repression.htm (17.08.2004)

« Les Cookies Démystifiés » www.tactika.com/cookie/cookie1.htm (01.09.2004)

« Comment ça marche ?» www.commentcamarche.net/internet/ftp.php3 (15.06.2004)

« La cryptologie » http://securinet.free.fr/cryptologie.html (06.09.2004)

« Cryptologie, moyen de sécuriser, les échanges » http://jurisexpert.net /site/fiche.cfm ?id_fiche=1213 (15.09.2004)

« Le Dico du Net » www.net-dico.com/termes/t.html

« Le Dico du web » www.olecorre.com

« Droits d'auteur » www3.teaser.fr/~jjrey/udp/97-98/Droits_d_auteur.html (14.07.2004)

« e-Europe » [1] http://europa .eu.int/scadplus/scad_fr.htm

« e-Türkiye » www.btvizyon.com.tr/viz_dergi_dosya .phtml (08.06.2004)

« Fikir ve Sanat Eserleri Kanunu » www.ilesam.org.tr/telif.html

« The French Net Dictionnary » www.geocities.com/paris/5587/dico.html

« Glossaire » [1] http://www.cjl.qc.ca/iabdd/iabdd2000/glossaire.htm (12.06.2004)

« Le Guide du web » www.zapilou.net/

« Hacking » www.cybercrimes.net/Property/Hacking/Hacking.html (23.12.2003)

« How Crackers operate? »
http://home.actlab.utexas.edu/aviva/compsec/cracker/howcrack.html
(23.12.2003)

« Histoire de l'İnternet »
www.chez.com/histoireinternet/internet_suite.htm (11.04.2004)

« İnternet ve Hukuk » www.superonline.com/hukuk/hukuk.htm

« İntroduction a l'encryptage »
http://membres.lycos.fr/nanaud/Encryptage/Introduction/intro.htm?
(06.08.2004)

« Jurisprudence sur la Netiquette »
www.forumetinternet.org/documents/jurisprudence/lire.phtml?id.260
(17.12.2003)

« La jurisprudence : quelques affaires marquante »
www.adbs.fr/site/publications/droit-info/mai.2000.pdf (05.05.2004)

« Meta Tag Lawsuits » http://searchenginewatch.com/resources/metasuits.html.
(09.12.2003)

« La Netiquette » www.cyberworkers.com/ledroit.fr/index-nétiquette.shtml

« Le Phénomène hacker » : www.ifrance.com/chamandine/ (19.12.2003)

« Phishing » www.infodunet.com/news/3465-phishing.html (02.09.2004)

« la pornographie infantile »
http://users.swing.be/criminologie/contenus/ch2/pornodown.htm. (17.08.2004)

« Pourquoi lutter contre le Spam ? »
http://www.caspam.org/spam.html (01.09.2004)

« Türk Ceza Kanunu Tasarısı » www.tcktasarisi.org

Prof. Dr. Köksal Bayraktar

Prof Dr Duygun Yarsuvat

Doç.Dr. Hatice Özdemir Kocasakal

Yrd. Doç. Dr. Ümit KOCASAKAL

Doç Dr. Idil KAYA
Galatasaray Üniversitesi
Sosyal Bilimler Enstitüsü