ITrust

# LES ASPECTS JURIDIQUES DU SCAN & DES TESTS INTRUSIFS

**OSSIR Journée Sécurité des Systèmes d'Information 2010**

I/ Prolégomènes / Quelques notions

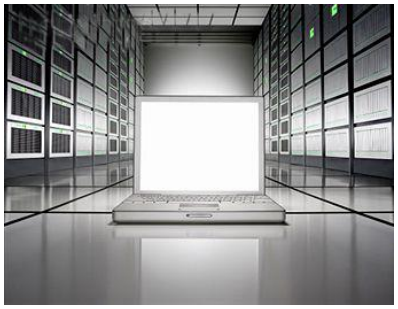
II/ L'Audit Intrusif & Expert en Sécurité informatique

III/ L'Informatique & Le Droit

IV/ L'Audit intrusif & Le Droit

V/ De la légalité du Scan

VI/ Autres Techniques de Sécurité ou de « Pirate » & Légalité



➔**Système d'information**

« Ensemble organisé d'éléments (*organisation, acteurs, procédures, systèmes informatiques*) qui permet de regrouper, de classifier et de diffuser de l'information sur un phénomène donné »

« Tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données »
*Convention Cybercriminalité 2001 Budapest*

➔**Information**

« Elément de connaissance susceptible d'être représenté sous une forme adaptée à une communication, un enregistrement ou un traitement ».
*Arrêté du 3 octobre 1984 du ministre de l'éducation et du ministre chargé des PTT*

➔**Système informatique**

« Partie automatisée d'un système d'information qui regroupe l'application de gestion et ses éléments d'accompagnement, les logiciels supports et les matériels.

➔**STAD, Système de traitement automatisé des données**

Tout équipement (*de nature matérielle, logicielle, ou "firmware"*) permettant l'acquisition automatique, le stockage, la manipulation, le contrôle, l'affichage, la transmission ou la réception de données.

Conception large : Réseau de France Telecom, réseau de Carte bancaire (*Trib. Correct. Paris, 25/02/2000*), un disque dur (*CA Douai, 7/10/1992*), un radiotéléphone (*CA Paris, 18 /11/1992*), un ordinateur isolé, un réseau local …

ITrust

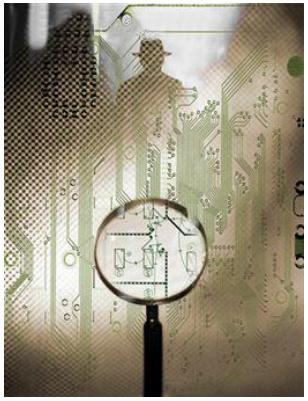
➔**« Hacker » / Pirate Informatique**

« Hacker s'introduit dans les systèmes par des moyens illégaux sans détruire les données ni utiliser les informations données, mais dans le seul but de faire savoir qu'il existe des failles de sécurité »
« Hacker » a l'origine : Programmeur passionné d'informatique / « Passer tout son temps devant son ordinateur … ».
« Hacking » : Synonyme de « Piracy » (contrefaçon) traité en droit français par CPI.

➔**« Cracker » (*casseur*)**

« Appellation qui désigne le pirate qui détruit dans un but précis ou pour le plaisir ».

➔**L'expert en sécurité informatique**



« Professionnel qui contribue à la mise en œuvre de la politique de sécurité de l'entreprise. Il fait remonter les risques en matière de sécurité informatique. Il met en place des contrôles de prévention en amont, de détection en simultané, d'explication et de consolidation en aval, pour contrer des intrusions ou des dysfonctionnements des systèmes informatiques. »

➔**Audit Intrusif**

« Prestation d'expert en sécurité informatique englobant plusieurs approches et méthodes dont l'objectif est d'évaluer le niveau de sécurité d'un système informatique ».

**« Face au « pirate » l'expert en sécurité informatique »**

➔**Méthode de « combat » devenir assaillant : Audit de Sécurité / Test intrusif**

Profilage, « social engineering : art of deception (L'art de la tromperie) », le scan de port, « l'exploitation » éventuelle des vulnérabilités …

Des audits en externe ou interne

- Audit Boîte noire *(Blind) / Architecture inconnue*
- Audit Boîte blanche */ Architecture fournie permet simulation de scénario*
- Audit sur Compte utilisateur */ Mesurer capacité nuisance interne : personnel malveillant ou négligence …*

➔**Finalité test d'intrusion :**

➢ **Eprouver la sécurité pour la renforcer**

- Mettre à l'épreuve la sécurité d'un environnement
- Qualifier sa résistance à un certain niveau d'attaque,
- Révéler des problèmes issus d'une incohérence entre différents composants
- Prouver que la sécurité mise en place est insuffisante

➢**Sensibiliser & Créer ou Renforcer :**

Politiques de sécurité / de Continuité ou de Reprise d'activité, charte informatique, etc.

Au niveau juridique : Intégrer des gardes fou dans les contrats (*clients, fournisseurs, prestataires, partenaires*).

➔La **Cyberdélinquance** (années 50, USA 1966, Finlande 1968)

➔La protection contre **l'espionnage**

- ✓ Espionnage de la NSA : logiciel «Promis», vente mondiale (Années 80-90)
  Intégration d'une puce électronique SMART (*Special Management Automate Resoning Tools*) piégeant le logiciel

- ✓ NSA : Logiciel ECHELON (1943-97 … )
  Système mondial d'interception des communications privées et publiques (SIGINT), élaboré par États-Unis, UK, Canada, Australie et Nouvelle-Zélande dans le cadre du traité UKUSA.
  Programme d'interception des e-mails, fax, télex et des communications téléphoniques via les réseaux de communications.

➔**Réaction de l'Etat Français**

- ✓ Réglementation en matière de protection des données
- ✓ Libéralisation du cryptage des informations de 40 à 128 bits en 1999 puis article 30 Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique « I. - L'utilisation des moyens de cryptologie est libre. »
- ✓ Lois sur le Terrorisme et Sécurité Intérieure / Loi d'Orientation et de Programmation pour la Performance de la Sécurité Intérieure (LOPPSI)

➔**Le respect des réglementations** exigence pour la sécurité des SI (Critères DICPR)

➔**Réglementations / Législations** & système d'information / informatique :

- ✓ Public varié (*Professionnels de l'informatique (DICPR) ou praticiens novices*)
- ✓ Multiples
- ✓ Complexes
- ✓ Nationales, Communautaires, Mondiales

➔**Droit Français** : Assimilation de « l'Informatique » dans le droit national

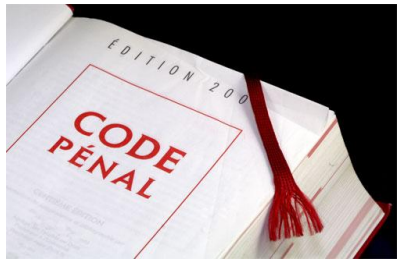
- ✓ **Législations généralistes / Droit commun :** *« Par tout support », « Quelque que moyen que ce soit » ou « commis par la communication au public en ligne »*
- ✓ **Législations spécifiques** : *Signature électronique, Droit du Producteur des BDD, Droit d'auteur des logiciels, Protection des données à caractère personnel « Informatique et Libertés », Loi Pour la Confiance en l'Economie Numérique, …*
- ✓ **Par des infractions spécifiques** *: Contrefaçon et P2P, Délit pénal de contournement des MTP, mesures techniques de protection, Usurpation d'identité numérique (LOPPSI II)*

… Et le régime de la Fraude informatique

➔**But Protéger Système informatique / « Système de traitement automatisé des données »**

➔**Loi Godfrain du 5 janvier 1988**, n° 88-19, code pénal : articles 323-1 à 323-7.
« Fraudes informatiques et atteintes aux systèmes d'information »

- ✓Délit d'accès non autorisé (Sanction : 2 ans / 30 000€ amende)
- ✓Maintien frauduleux dans un système informatique
- ✓Entrave et/ou fausse le fonctionnement d'un système de traitement automatisé
- ✓Introduit frauduleusement des données dans un système d'information ou les modifie, ou les supprime (Sanction : 3 ans / 45 000€ amende)




➔**Eléments constitutifs :**
✓ Intrusion dans le SI : Sanctionnée qu'elle soit réalisée sur le moniteur même ou à distance, que le maintien ait eu lieu après accès fortuit,
✓ Signification de « Frauduleusement » : Volonté de s'introduire **ou** de se maintenir sans droit

➔**Régime**

- ✓ La tentative est punissable (article 323-7)
- ✓ Les personnes morales sont condamnables (article 131-39)
- ✓ Le recel après fraude informatique est condamnable (information / identifiants …)

➔**Un test d'intrusion commence par une reconnaissance :**

✓ Récupération d'infos (noms de domaines, Google, société.com, ...)
=> Pas de difficulté notable, consiste en une récolte de données publiques

✓ Scan protocolaire (déterminer pour chaque machine les protocoles de transport fonctionnels : TCP, UDP, ICMP, ...)

✓ Scan de ports TCP, UDP (déterminer quels ports sont ouverts, fermés ou filtrés (firewall))

➔**De la reconnaissance à l'identification :**

✓ Identification des systèmes d'exploitation (LINUX, BSD, WINDOWS, ...)

✓ Identification des services ainsi que de leur version (Ex: port 80, serveur Apache, version xxx).

➔**De l'identification à la recherche de vulnérabilité :**

✓ Identification de vulnérabilités (Ex par utilisation de NESSUS. )

✓ Exploitation éventuelle des vulnérabilités

# IV/ Légalité du Pen test

➔**Le Pen test :**

- ✓ Test applicatif : Recherche de vulnérabilités et de l'exploitation de failles
- ✓ Eventuellement test poussé jusqu'à compromission machines (direct ou par rebond)

➔**Les Risques :**

- ✓Le Déni de Service
- ✓L'atteinte à la confidentialité
- ✓Les droits de Propriété intellectuelle et / ou Industrielle
- ✓Etc.

➔**Consiste en un accès illégal au STAD ?**

NON si autorisation explicite

⇒Le réflexe contrat et NDA

⇒Le strict respect des autorisations contractuelles

**L'autorisation et les contrats permettent la Maîtrise des Risques**

Protection du prestataire de Sécurité : Clause limitative ou élusive de responsabilité (Sous couvert de Bonne foi (*art. 1134 al. 3 du Code civil*) et à défaut de tout dol (erreur) ou faute lourde).

**Jurisprudence :**

L'autorisation rend l'intrusion licite

- ✓L'infraction n'est pas constituée en présence d'une habilitation (*Grenoble 2002*)
- ✓Le retrait d'habilitation, après accès, rend le maintien dans le SI illégal (*Paris 5 avril 1994 : D. 1994. IR. 130 ; JCP E 1995. I. 461, obs. Vivant et Le Stanc …*)

ITrust

➔**Condamnations :**

- ✓ **Abus de confiance**, Stagiaire chinoise. *Mais pas pour intrusion ou accès STAD (TGI de Versailles, 18/12/2007)*
- ✓ **Violation** du **secret des correspondances**, **accès frauduleux** à un **SI** & **Recel** des **informations** (*TGI Paris, 12ème chbre, 01/06/07, O. et Cie contre Thrinh Nghia T. et Trung T*)
- ✓ **Usurpation mot de passe / violation charte informatique** (*Cass, le 21/12/06, Monsieur P. contre société Ad 2 One SA*)
- ✓ **Maintien frauduleux** dans un SI : Neutralisation de la déconnexion automatique (*Tribunal Correct. Paris 1996 « Rafraîchissement d'écran »)*
- ✓ **Maintien illégal après Accès régulier**, pendant + 2 ans, à une BDD avec un code remis pour une simple période d'essai (*Cass. Crim 3/10/2007*)

➔**Relaxes :**

- ✓ Si le système n'est **pas protégé** et si celui qui le maîtrise n'a **pas manifesté sa volonté d'en limiter l'accès** : Pas d'infraction (*Paris 08/12/1997, Gaz Pal. 1998. 1, chron. Crim. 54*)
- ✓ Pas de délit de Maintien frauduleux dans un SI quand le **site peut-être atteint par un logiciel grand public de navigation** (*CA Paris, 11ème Chambre, 8 décembre 1997 & CA Paris, même Chbre. 30 octobre 2002 « Kitetoa »)*
- ✓ Ainsi qu'hypothèse d'autorisation explicite (contrat)

➔**Signature de la Convention sur la Cybercriminalité de Budapest (2001)**
Objectif mener « une politique pénale commune destinée à protéger la société de la criminalité dans le cyberespace, notamment par l'adoption d'une législation appropriée et par l'amélioration de la coopération internationale ».

Infractions contre la confidentialité, l'intégrité et la disponibilité des données et SI à adopter par les Etats dans leur droit interne :

- ✓Art.2: **Accès illégal** (intentionnel et sans droit / Option violation mesure de sécurité)
- ✓Art.3: Interception illégale (intentionnelle et sans droit)
- ✓Art. 4: Atteinte intégrité des données (Intention, sans droit / Option do sérieux)
- ✓Art. 5: Atteinte intégrité Système (entrave grave, intention, sans droit)
- ✓Etc.

43 États signataires dont les États-Unis, le Japon, l'Afrique du Sud et le Canada
France : entrée en vigueur 2006 (adoption du décret du 23 mai 2006)

➔**La plupart des pays,** même non signataires :
Infraction d'intrusion SI : ***Brésil, Turquie, Chine, Russie, Maroc*** …
*=> pas infraction sur interceptions illégales pour les deux derniers*

*Source : Conseil de l'Europe Project on Cybercrime www.coe.int/cybercrime*

➔**Convention sur la Cybercriminalité de Budapest (2001)**

*Objectif mener « une politique pénale commune destinée à protéger la société de la criminalité dans le cyberespace, notamment par l'adoption d'une législation appropriée et par l'amélioration de la coopération internationale ».*

➔**Rappel le choix d'opter pour élément constitutif « Présence ou violation d'un dispositif de sécurité »**

- ✓ **Lois étrangères le retenant :** Norvège, Finlande, Pays Bas, Suisse, Luxembourg …
- ✓ **D'autres**, comme la France, **n'exige pas cette condition** : Canada, Danemark, Royaume-Uni, Australie …

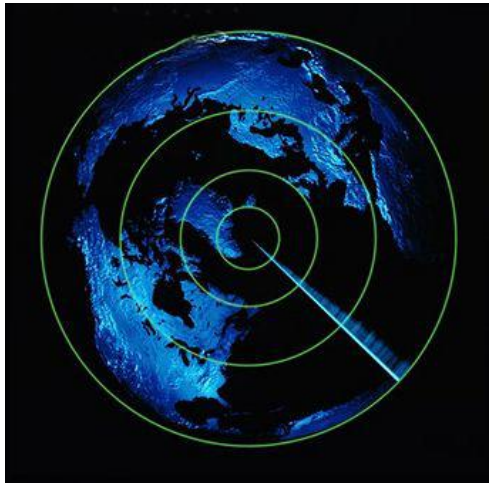
**France :**

« La protection d'un système de traitement automatisé de données par un dispositif de sécurité n'est pas une condition de l'incrimination. »
*Cour d'appel de Toulouse, dans un arrêt du 21/01/1999*
*Jugement 31ème chambre correctionnelle du TGI Paris 18/09/2008*

*Source : Conseil de l'Europe Project on Cybercrime www.coe.int/cybercrime*

**Le Scan de Port : Vue d'ensemble**

✓ Découvrir l'architecture / les services de la cible (*routeurs et firewalls, relais applicatifs, répartiteurs et fermes de serveurs*).
Opération de balayage des ports (1 à 65535)



✓ Une « *technique consistant à balayer automatiquement à l'aide d'un programme approprié, une série d'adresses IP spécifiques afin de trouver et d'examiner les ports ouverts sur chaque ordinateur, (…)* »

➔**Des outils :**

✓ Hping (envoie de paquet vers port TCP – Réponse indique existence Port. Scan. Traceroute applicatif)

✓ Nmap (détecter port ouvert et identification service)

✓ Scapy (Scan. Traceroute applicatif. Et Pen test. Générer Paquet / Mais aussi intercepter paquet)

➔**Les ports :** « portes » / accès par lesquels une machine communique et échange des informations avec d'autres machines.

➔**Approche pratique : Analogie possible avec la notion de domicile, n° téléphone …**
Informations collectées sont de caractère « public »
*(« Le scan de ports : une intrusion dans un STAD ? » Xavier LEMARTELEUR, juriste spécialisé en droit des technologies de l'information*)

**Scans en détails**

➔ **Scan protocolaire** (déterminer pour chaque machine les protocoles de transports fonctionnels : TCP, UDP, ICMP, ...)

=> A ce niveau : Scan consiste à vérifier existence des protocoles de transport et non de leur utilisation effective.

Expert en sécurité :
Niveau 4 couche OSI. Faible risque de DoS. Pas d'accès au SI. Simple envoie de paquet pour réponse

Droit : Pas introduction, suppression ou altération données du SI. Intrusion / entrave SI ?

➔ **Scan de ports TCP, UDP** (déterminer quels ports sont ouverts, fermés ou filtrés (firewall))

=> Scan consiste à déterminer que les ports sont ouverts mais sans confirmer que le port est dédié à l'application supposée.
Scan : Protocole TCP : OK, Port 80 ouvert mais pas identifié si HTTP.

Expert en sécurité :
Niveau 7 couche OSI. Faible risque de DoS. Pas d'accès au SI. Simple envoie de paquet pour réponse.

Droit : Pas introduction, suppression ou altération données du SI. Intrusion / entrave SI ?

➔ **Identification des systèmes d'exploitation** (LINUX, BSD, WINDOWS, ...)

=> A ce niveau : Envoie de paquet pour réponse. Paquets reçus, informations plus pertinentes.

Expert en sécurité :
« Ce n'est pas une requête habituelle ». Une 10aine de paquet Nmap envoyés, les réponses reçues permettent identification des SE.
Cependant aucune action réalisée, juste information. Pas d'accès au SI.

Droit : Pas d'intrusion ou entrave, ni introduction, suppression ou altération données du SI.

➔ **Identification des services ainsi que de leur version** (Ex: port 80, serveur Apache, version xxx).

Expert en sécurité :
Niveau 7 OSI. Opération opérant un transfert de données. Requête au niveau du Service donc un accès. Test des services applicatifs. Risque de DoS.
Permet identifier existence et utilisation application FTP, Apache sur le protocole HTTP permettant de visualiser des pages WEB, port 80 …

Droit : Pas introduction, suppression ou altération données du SI. Intrusion / entrave SI ?

➔ **Des éléments de réponse :**

**L'existant : Loi Godfrain**

Art 323-3-1 Code pénal, Loi n°2004-575 du 21 juin 2004 - art. 46 JORF 22 juin 2004 :
« *Le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée* »

Texte, initialement conçu pour lutter contre la détention volontaire de programmes d'origine virale.

**Applicable cependant à la simple détention de logiciels de scans** : Une présomption d'intention d'intrusion et autres infractions d'atteintes aux STAD.
Condition : « Sans motif légitime ». Or objectif possible : Sécurisation des réseaux.

➔ **Réflexion sur la Pratique du Scan : Un acte préalable à une Attaque ?**
**Décembre 2005, Chercheurs de l'Université du Maryland :**
Un simple scan de port n'aboutit que très rarement à une attaque malveillante
Seulement 5 % des attaques sont précédées d'un scan de port classique

Tendance : Scan mono-port et Worldwide (Ex : port 21 FTP ou 25 SMTP sur un pull ip).

➔**Article 6 Convention sur la Cybercriminalité de Budapest (2001)**

La production, vente, obtention pour utilisation, importation, diffusion ou d'autres formes de mise à disposition ainsi que la **possession** *d'un dispositif, y compris un programme informatique, principalement conçu ou adapté pour permettre la commission d'infractions*

**Sont des Infractions sauf :**

- ✓Si dépourvu de Volonté / d'Objectif de commettre une infraction
- ✓Si dans le cas d'essai autorisé ou de protection d'un système informatique

Harmonie internationale législative sur cette approche

# V/ Légalité du Scan de port
# ... À l'étranger

ITrust

➔ **USA**

Scan pas sanctionné :
Quand il ne permet pas d'accéder au réseau & que les données ne sont pas en danger.
*US district court of Georgia, Moulton v. VC3, 2000 WL 3331091 (N.D. Ga., Nov. 7, 2000)*

Droit Américain (jurisprudence et législation) sanctionne l'intrusion quand :

- ✓ Elle s'accompagne d'une utilisation non autorisée
  ET
- ✓ Inflige de dommages sur l'ordinateur et qu'il y ai **intention** de commettre un délit.

=> *S'entend aussi du simple fait de s'approprier des informations protégées*

**Cadre législatif :**
The Computer Fraud and Abuse Act
*Sanction : Amende, Prison (jusqu'à 20 ans dans certains cas)*

**A retenir :**
Etats-Unis existence Infraction autonome du commerce des mots de passe et informations (similaires) permettant accès sans droit aux système d'information

➔ **ISRAEL**

Relaxe de l'auteur d'un Scan du site web du Mossad poursuivi pour tentative d'accès non autorisé.
*Hon. Abraham N. Tennenbaum (2004-02-29). "Verdict in the case Avi Mizrahi vs. Israeli Police Department of Prosecution.*

Juge :
« D'une certaine manière, les internautes qui vérifient les vulnérabilités des sites Web agissent dans l'intérêt public. Si leurs intentions ne sont pas malicieuses et ils ne causent pas de dommages, elles doivent même être félicitées »

Législation israélienne & infractions informatiques : **The Computers Law of 1995**

➔ **CHINA**

Mauvaise publicité « affaire Google-Chine »
Puis Opération répressive et médiatique « Black Hawk Safety Net » (fév. 2010)
*Arrestation d'un réseau de Hacker pour mise à disposition d'outil de hacking / Formation au piratage (12000 membres)*. Fermeture site web.

➔**Cadre législatif**

Loi pénale 2009 chinoise (ajout récent) « : *Interdit aux particuliers de concevoir, d'offrir ou de vendre des programmes pirates en ligne au prétexte qu'ils pourraient être utilisé pour des actes de cybercriminalité* ».

*Le « Scan » = outils de piratage ? Pas d'information claire*
*Autres outils cependant OUI*

Articles of "**Criminal Law of the People's Republic of China**" : (code pénal chinois)

- ✓Art. 252 : Illegal interception (équivalence violation correspondance privée) (1 an)
- ✓Art. 285 : Illegal access computer systems … (3 ans emprisonnement)
- ✓Art. 286 : Illegal alteration, add, interfere or delete. (5 ans)
  - ⇒*Provoquant dysfonctionnements des systèmes et conséquences graves*
  - ⇒Concerne SI, Data & aussi création et **propagation outil de piratage (virus, etc)**

*Industrie Piratage en Chine = 7,6 milliards de yuans  pertes (1,1 milliards de dollars) en 2009*

## L'approche Européenne

Plus strict : La pénétration au SI est un « crime » indépendamment de tout dommage causé (*également adoptée par d'autres pays*)

➔**Finlande**

Cour suprême confirme verdict Cour Appel condamnant un JH de 17 ans pour intrusion dans le SI d'une banque finlandaise (balayage port réseau) 1 an emprisonnement et amende.

Amende + 12000€ de dédommagements pour couvrir frais importants enquête par la banque. Esa Halmari Attorney (2003), Retrieved 2009-05-07.

➔**Angleterre**

Insertion nouvel article dans "the Police and Justice Act 2006" (Act of the UK Parliament). Illégal « fournir ou d'offrir de « l'offre » susceptible d'être utilisé pour commettre, ou pour aider à la perpétration d'une violation à la "Computer Misuse Act 1990" ».

Régime : 6 mois à 5 ans d'emprisonnement et amende. Elément intentionnel.

➔ **Allemagne**

**Cadre légal**
Section 202c StGB of the computer crime laws (Code Pénal allemand) :

Interdiction de « posséder, vendre, distribuer, créer, utiliser des logiciels qui pourraient être utilisés (potentiellement) comme outils de piratage ».

« La simple possession d'outils … permettant recueillir ou d'accéder à système d'information … est un crime ». 12 mois d'emprisonnement et amende.

**Jurisprudence**
Aucune poursuite à ce jour ;
Recherche en sécurité de SI a été ébranlée : abandon de nombreux projet de recherche.

Décision de la Cour constitutionnelle fédérale allemande, la sanction légale ne s'applique que dans le cas où le logiciel a été développé avec l'intention illégale à l'esprit (*18. Mai 2009*)

***A noter*** *l'évolution récente du droit Allemand en matière de conversation des données de connexion censurée par la Cour Constitutionnelle Allemande.*
*Manque de sécurité et restrictions insuffisantes en termes d'accès à ces données.*

# V/ Le Scan de Port : Illégal ?

➔ **Deux approches :**
Elément intentionnel plus déterminant que jamais

- Illégalité du scan
  - ✓Le Scan est une étape préalable à une infraction (présomption)
  - ✓ Le Scan est un accès frauduleux
    - *Induit une volonté de s'introduire ou de se maintenir*
    - *Induit un défaut d'autorisation lors de l'intrusion ou du maintien*

- Légalité du scan
  - ✓Le Scan n'est pas présumé acte préparatoire à une infraction
  - ✓Le Scan n'est pas un accès à un SI ou une tentative

➔ **Légalité du Scan de Port ?**

⇒La Réponse viendra des Juges
⇒Pas de précédant en droit Français :
*Quelques pistes (Décision Kitetoa et autres)*

➔**Solution ?**
**Anticiper sur le contentieux** : Se prémunir d'autorisation & Respecter le cadre contractuel

➔ **De l'identification à la recherche de vulnérabilité**

**Vulnérabilités** : *Faiblesses de conception, de mise en œuvre ou de l'utilisation d'un composant matériel ou logiciel du système.*

**Exploitation éventuelle des vulnérabilités : solution simple**

⇒*Exemples :*

- ✓ *Prise de contrôle d'un système / d'une machine par un accès Root*
- ✓ *Exécuter des commandes sur le système hébergeant l'application*
- ✓ *Planter un serveur ou un réseau*

Illégale si dépourvue d'autorisation : L'exploitation consistant à un accès ou une modification, suppression ou altération des données et risque de DoS.

**Identification de vulnérabilités : ambiguïté de la solution**

*Par la comparaison SE et versions applications avec BDD de vulnérabilités (type Nessus).*

- ✓ Pas d'illégalité : ne consiste pas en un accès à un STAD
- ✓ **Quid** cependant de la présomption / acte préalable d'une infraction ?

**Problématiques des publications des « vulnérabilités »**

-Full Disclosure => Délit pénal (323-3-1 code pénal) & Contrefaçon + Confidentialité

-Obligation publication des «atteintes aux traitements de données à caractère personnel» (FAI & opérateurs télécom) *(La sécurité des données personnelles enfin prise au sérieux ? Bruno Rasle, février 2010)*

# VI/ Légalité du “ Sniffing ”

➔ **Sniffing** « écoute » d’un réseau et des paquets qui transitent (Résolution problématiques de sécurité réseau)

➔ **Logiciel de Sniffing**, packet sniffers ou « renifleurs de paquets » : TCPdump, Wireshark Pas intrusif ; mais récupération info confidentielle.

Permettent consultation aisée : données non-chiffrées et intercepter mots de passe qui transitent en clair ou toute information non-chiffrée ….

✓ **Ecoute passive : Article 226-15 du code pénal**

1 an emprisonnement et de 45000€ d'amende.
- Le fait, commis de mauvaise foi, d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivées ou non à destination et adressées à des tiers, ou d'en prendre frauduleusement Connaissance.
- Le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie des télécommunications ou de procéder à l'installation d'appareils conçus pour réaliser de telles interceptions.

✓ **Ecoute active :**

Ajout d’information dans les paquets ou modification de certains messages => Loi Godfrain

➔**Préconisation** :

Autorisation même si écoute passive

➔ **Sniffing,** « écoute » du réseau/des paquets, **une Interception illégale des informations ?**


Art. 3 Convention cybercriminalité Budapest
Interception illégale de données informatique : Intention, sans droit, lors de transmission non publiques.

**« Le terme 'non publique' qualifie la nature du moyen de transmission (communication), non la nature des données transmises … mais n'exclut pas en soi les communications par le biais des réseaux publics ».**

*Source : « Convention sur la cybercriminalité : Peut-on coordonner l'action de la justice? » auteur Thibault de Manoir de Juaye avocat.*

⇒**Infraction qui vise interception illégale pour :**

- ✓ Information sur un réseau de communication non-publique
- ✓ Information confidentielle / « secrète » sur un réseau public

*Interception sans droit en vertu de l'article 3 (voir, par exemple, l'arrêt rendu par la CEDH dans l'affaire Halford c. Royaume-Uni, 25 juin 1997, 20605/92)*

➔**Préconisation : Dans le doute du caractère « public » obtenir l’autorisation**

➔**Rappel**

Pays comme le Maroc ou la Russie pas d’infraction sur l’interception illégale.

## Contexte :

- ✓ Incrimination quand « sans droit » et acte intentionnel
- ✓ Présomption d'intention de certains actes si acte préalable à une incrimination
- ✓ Difficulté de la preuve
- ✓ Réglementation généraliste
- ✓ Jurisprudence inexistante ou contradictoire

## Préconisations :

### S'enquérir d'autorisation / contrat

- ✓ Dans toutes les opérations d'audit intrusif
- ✓ Valider toutes les phases : Scan de port - Exploitation des vulnérabilités
- ✓ Même les actes de sniffing & même si écoute passive
- ✓ Valider les plannings / délais
- ✓ Information sur les risques et déterminer les responsabilités éventuelles

### Améliorer la « culture » Sécurité

- ✓ Associer les compétences techniques et juridiques
- ✓ Désignation de CIL
- ✓ Sensibilisation des users …

➔Remerciements
à l'OSSIR et ses représentants
à Denis Ducamp, Consultant Sécurité SI
à tous les Auteurs de travaux sur le thème

Questions

Yoann Garot | Chef de Projet Innovation & Service Juridique / Innovation Project Manager & Lawyer
Mel. y.garot@itrust.fr & yoanngarot@gmail.com | 06.64.27.89.92

ITrust | Immeuble ACTYS/1 Avenue l'Occitane BP 67303 | 31673 LABEGE CEDEX
Fixe Sdt. 09.80.08.36.12| Fax. 09.80.08.37.23 - contact@itrust.fr
http://www.itrust.fr | Assurance intégrité | Cabinet de conseil en sécurité informatique