Introduction au droit de la sécurité des systèmes d'information

L'essor de l'internet a renouvelé les problématiques juridiques en raison de son caractère transnational et soulève de nouveaux problèmes de sécurité propres aux risques d'intrusion spécifiques au commerce électronique, aux risques d'espionnage industriel ou encore aux sabotages.

La cyberdélinquance s'est professionnalisée.
Ce n'est désormais plus seulement le fait de jeunes étudiants en mal de notoriété, mais, bien souvent, de techniciens intégrés à un écosystème mafieux, complexe et occulte.

Avant d'aborder le droit de la sécurité des systèmes d'information stricto sensu (B) il convient d'envisager les différents types de cyberattaques (A). Cela permettra de mieux apprécier la façon dont le législateur a décidé de sanctionner judiciairement les auteurs de ce type de délits.

A. Différents types de cyberattaques

Les cyberattaques sont variées et rivalisent, bien souvent d'ingéniosité.

1. Les virus

Ce sont des programmes cachés dans un fichier dont le double but est de s'intégrer dans le système d'exploitation de l'ordinateur et de se propager à d'autres.
Cela peut avoir pour conséquence de détruire toutes les données présentes sur le disque dur.
On fait parfois la distinction entre les virus et les retrovirus. Ces derniers sont justement conçus pour entraver l'action des logiciels antivirus.

2. Les vers

Ce sont, à l'inverse des virus, des programmes autonomes.
Ils entrainent la destruction de données, le détournement d'informations confidentielles ou encore le simple arrêt de l'ordinateur qui a été infecté.
Les vers ou worms en anglais disposent, comme les virus, d'une capacité d'auto-reproduction qui est à la base du phénomène de propagation. A la différence du virus, il ne contamine aucun élément de l'ordinateur sur lequel il s'installe.
Il existe des moyens techniques pour procéder à la décontamination d'un ordinateur par un vers.

3. Les chevaux de Troie

Ce sont des programmes prenant l'apparence d'un programme normal, trompant ainsi les systèmes de sécurité, pour pénétrer dans des fichiers.

Ces chevaux de Troie peuvent servir à la capture d'informations personnelles (mot de passe, identifiants, etc…) à la destruction de fichier ou encore au déclenchement d'attaques ciblées par envoi de mails (spams).

Ce type de virus, comme son nom l'indique, est introduit à l'insu de l'usager. Il se présente sous la forme d'un fichier le plus souvent exécutable (.exe) ; fichier qui vient s'installer sur le disque dur et qui est programmé pour déterminer une configuration visant à permettre au pirate de prendre le contrôle de la machine à distance.

Le PC victime ouvre alors une porte vers l'internet, laquelle permet au pirate qui a programmé le « Cheval de Troie » de se connecter vers ladite machine et d'y effectuer une multitude de transactions (les plus connus Back Office, Net Bus, Magic Lantern, Dlder).

4. Les attaques contre les sites

Ces attaques peuvent se faire par saturation, soit par altération.
La saturation consiste pour les pirates informatiques à envoyer à des milliers d'ordinateurs, via internet, des chevaux de Troie « dormants » programmés pour se déclencher à un jour J ou activés à distance, contre un site précis (DOS).

A titre d'exemple, en Estonie, le 27 avril 2007 les sites gouvernementaux et bancaires ont été bombardés à raison de 2 000 visites par seconde.

L'altération (defacing ou defaçage) consiste à attaquer un site par une porte dérobée ou par un logiciel espion, puis à modifier son contenu à l'insu de ses administrateurs.

L'objectif poursuivi par les pirates par une telle intrusion dont est victime le site internet de l'entreprise est de nuire à son image de marque. Il s'agit également de générer un défaut de performance ou une absence de disponibilité.

Sa page d'accueil originale se trouve supprimée au profit d'une page de leur cru.

Il s'agit d'une attaque comportant trois éléments :

- Un message à caractère technique, humoristique, politique ou sexuel

- Une revendication qui tente d'expliquer les motivations réelles ou non des pirates quant au choix du site attaqué
- une signature qui est une marque promotionnelle

Il existe un second type d'attaque au cours de laquelle les pirates se contentent de construire un second site internet, sous leur contrôle, et dont le contenu peut n'avoir aucun rapport avec le site original.

Il existe différents types d'attaques possibles ayant pour effet de porter atteinte à la sécurité du réseau d'un site internet

1. *Le scan qui balaye chaque port IP afin de connaître les services offerts par le système*
2. *Le spoofing visant à utiliser l'adresse IP d'une machine pour s'introduire sur le réseau d'une entreprise*
3. *Le sniffing qui est une méthode consistant à écouter le réseau afin d'intercepter des logins et mot de passe.*
4. *Le crack de mots de passe qui consiste pour le hacker à prendre une série de lots qui lui semblent pouvoir correspondre au mot de passe et comparer le résultat encrypté au mot de passe stocké par la machine.*

5. **Les logiciels espions (ou spywares)**

C'est un ensemble de programmes s'installant dans l'ordinateur. Ces logiciels servent à récupérer puis à envoyer via internet des informations personnelles au concepteur ou à l'utilisateur du logiciel espion.
Le spyware n'est pas techniquement un virus. Il n'exploite pas les failles de sécurité présentées dans les systèmes d'exploitation pour se diffuser.

Ils sont très souvent intégrés à des logiciels et une fois installés sur l'ordinateur de l'utilisateur, ils vont surveiller et enregistrer l'utilisation qui en est faite et envoyer des informations aux opérateurs qui ont financé la diffusion de ce programme espion.

6. **Le spam**

Le spam se définit comme une communication non sollicitée envoyée en masse par internet.
L'envoi normal est celui dans lequel le spammer passe par un serveur de mail qu'il a l'autorisation d'utiliser.
Cela peut être une entreprise qui dispose d'une ligne louée avec son propre serveur de mail.

En pratique, il est très difficile de se protéger de la réception du spam, car plus les contraintes de filtrage sont importantes, et plus les risques de bloquer du courrier légitime augmentent.
Il existe, par exemple, des solutions fondées sur l'adresse IP du serveur distant. Elles consistent à filtrer les communications sur la base du contenu du message.

7. L'hameçonnage

Le phishing ou hameçonnage est une technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité. La technique consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance — banque, administration, La Poste France Télécom, etc. — afin de lui soutirer des renseignements personnels : mot de passe, numéro de carte de crédit, date de naissance, etc.

Il s'agit par exemple d'usurper un site bancaire pour abuser ses utilisateurs.

Cela peut passer par un courriel malveillant dans lequel un pirate envoie un courriel à une victime potentielle en se faisant passer pour sa banque.

Il s'agit parfois de faux sites créés pour l'occasion. En cliquant sur le lien contenu dans le courriel, la victime arrive sur un faux site web, ressemblant au site de la banque de la victime. Elle remplit alors un formulaire en donnant l'identifiant du compte et le mot de passe.
Il peut aussi s'agir de détournement de fonds. Les pirates ponctionnent alors les comptes de leurs victimes au profit de comptes qui sont sous leur contrôle.

Il arrive très souvent que des milliers d'internautes reçoivent un message prétendument urgent indiquant que le département technique d'une grande banque dont ils sont clients souhaite procéder à une mise à jour de logiciels (ou encore à un remboursement d'une somme perçue par erreur) de façon à améliorer la qualité des services bancaires en cliquant sur un lien et en confirmant leurs détails bancaires.

C'est une forme d'attaque informatique reposant sur l'ingénierie sociale. Elle peut se faire par courrier électronique, par des sites web falsifiés ou autres moyens électroniques.

De façon générale, les entreprises veulent avoir l'assurance que leurs données confidentielles sont protégées et en sécurité lorsqu'elles transitent par l'internet.

Elles veulent également avoir la garantie que, ni les ordinateurs, ni leurs réseaux ne seront exposés à des risques du fait de leur connexion à internet.

Les utilisateurs veulent être certains que les données qu'ils reçoivent sont bien les mêmes que celles qui leur ont été envoyées (aucune altération du document lors de son transit entre l'ordinateur de l'expéditeur et celui du destinataire).
Ils veulent également avoir l'assurance de la légitimité du site internet qu'ils visitent.

Il existe traditionnellement 5 voies de contamination des systèmes d'information

1. Les sites web sont susceptibles d'être infectés par les chevaux de Troie et les logiciels espions

2. Les téléchargements sont la porte d'entrée aux chevaux de Troie et aux logiciels espions

3. Les courriels sont vecteurs de virus, de vers et de chevaux de Troie

4. Les réseaux (ordinateurs connectés entre eux) peuvent être infectés par des vers

5. Les périphériques, CD ROM, DVD, disquettes et clé USB peuvent transmettre les vers, virus, chevaux de Troie et logiciels espions.

Les différentes cyberattaques que nous venons d'évoquer mettent l'accent sur la nécessité que puisse exister, outre une politique de sécurité mise en place par l'entreprise, des réelles sanctions judiciaires à l'encontre de ceux qui seraient les auteurs de ces délits.

B. Le droit de la sécurité des systèmes d'information

Le parc informatique des entreprises est de plus en plus exposé aux attaques numériques parmi lesquelles l'espionnage industriel, le hacking ou le vol de données ne sont que quelques exemples.

Selon un article de feu le quotidien La Tribune[1], les pertes de données liées à des actes de piratage ont coûté en moyenne 2,2 millions d'euros aux entreprises visées par ces attaques en 2010.

Quid de la cybercriminalité ?

La cybercriminalité peut être séparée en trois catégories d'activités :

1) Les formes dites traditionnelles de criminalité comprennent le vol, l'escroquerie et la pédopornographie

2) La publication de contenus illicites par voie électronique (pédopornographie, documents protégés par le secret professionnel, contrefaçon, etc…)

3) Les infractions propres aux réseaux électroniques à savoir les attaques visant les systèmes informatiques, le *déni de service (saturation)* et le piratage.

   Une attaque par déni de service (Denial of Service Attack, ou DoS) est une attaque informatique ayant pour but de rendre indisponible un service, d'empêcher les utilisateurs légitimes d'un service de l'utiliser.

   Il peut s'agir de :

   - l'inondation d'un réseau afin d'empêcher son fonctionnement ;
   - la perturbation des connexions entre deux machines, empêchant l'accès à un service particulier ;
   - l'obstruction d'accès à un service à une personne en particulier.

C'est majoritairement le droit pénal qui donne les moyens de lutter contre ce type d'agissements et de sanctionner leurs auteurs.

[1] « La cybercriminalité, un business à 1.000 milliards », 28 juin 2011.

Le droit pénal et la protection des systèmes informatiques

Le droit français et le Code pénal en particulier ont instauré un dispositif répressif destiné à lutter contre la cybercriminalité.

De façon générale, le droit n'a pas vraiment vocation à distinguer l'identité du responsable de l'atteinte, si celle-ci est avérée et que son responsable n'a pas autorité pour le faire.

Nous allons envisager le dispositif répressif destiné à lutter contre cette nouvelle forme de criminalité.

L'apport de la loi Godfrain

La loi n°88-19 du 5 janvier 1988 relative à la fraude informatique dite Loi Godfrain en est la pierre angulaire de la lutte contre la criminalité informatique.

Elle a mis en place les articles 323-1 et suivants du Code pénal qui traitent de la fraude informatique.

Ces articles ont été modifiés par la loi n°2004-575 du 21 juin 2004 dite Loi de Confiance dans l'Economie Numérique.

1) La répression du Hacking (L'incrimination d'accès ou de maintien frauduleux dans un Système de Traitement automatisé de Données (ou STAD).

L'article 323-1 du Code pénal[2] sanctionne la pratique du hacking.
Il rend les intrusions dans un système de traitement automatisé de données passibles de deux ans d'emprisonnement et de 30 000 euros d'amende.

L'alinéa 2 de ce même article prévoit une aggravation de peine lorsque l'accès frauduleux au système a entrainé la suppression ou la modification des données ou l'altération du fonctionnement du système. 3 ans d'emprisonnement et de 45 000 euros d'amende.

Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel

---

[2] Article 323-1 du Code pénal, Modifié par LOI n°2012-410 du 27 mars 2012 - art. 9 : *« Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30000 euros d'amende.*
Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45000 euros d'amende.
Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à cinq ans d'emprisonnement et à 75 000 € d'amende ».

mis en œuvre par l'Etat, la peine est portée à cinq ans d'emprisonnement et à 75 000 euros d'amende.

L'accès frauduleux est constitué dès lors qu'une personne non habilitée pénètre dans un système de traitement automatisé de données tout en sachant qu'elle est dépourvue d'autorisation. C'est ainsi qu'un groupe de hackers a été condamné pour s'être introduit sur le site Internet de la Mission interministérielle de lutte contre la drogue et la toxicomanie. (CA Paris, 28 janv. 2010)

La différence entre un accès et un maintien frauduleux dans un STAD.

Une affaire récente illustre cette différence.

Elle opposait un certain Olivier L. au ministère public. (*Cour d'appel de Paris Pôle 4, chambre 10 Arrêt du 5 février 2014).*

Il était reproché à Olivier d'avoir accédé et de s'être maintenu, par le biais d'une recherche Google dans l'extranet de l'Agence Nationale de Sécurité Sanitaire de l'Alimentation, de l'Environnement et du Travail (Anses), lequel était insuffisamment sécurisé. Il lui était également reproché un vol des données auxquelles il a accédé.

L'analyse des journaux de connexions a permis de remonter jusqu'à lui via un VPN détenu par la société dont il était le dirigeant.

S'il a affirmé aux autorités judiciaires être arrivé "par erreur" au cœur de l'extranet de l'Anses, il avait reconnu « *avoir parcouru l'arborescence des répertoires de celui-ci et être remonté jusqu'à la page d'accueil sur laquelle il avait constaté la présence de contrôles d'accès (authentification par identifiant et mot de passe)* ».

La Cour d'Appel ne l'a pas reconnu responsable d'un accès frauduleux au motif qu'il n'était pas établi « *suffisamment par les pièces de la procédure que le prévenu s'est rendu coupable d'accès frauduleux dans un système de traitement automatisé de données ; que l'accès, qu'il ne conteste pas, lui a en fait été permis en raison d'une défaillance technique concernant l'identification existant dans le système, défaillance que reconnaît l'Agence Nationale de sécurité sanitaire de l'alimentation, de l'environnement et du travail ; que dans ces conditions l'infraction n'est pas caractérisée* ».

En revanche, concernant le délit de de maintien frauduleux dans un système de traitement automatisé de données et de vol, elle a retenu « *qu'il est constant que le système extranet de l'Agence Nationale de sécurité sanitaire de l'alimentation, de l'environnement et du travail n'est normalement accessible qu'avec un mot de passe dans le cadre d'une connexion sécurisée, que le prévenu a parfaitement reconnu qu'après être arrivé "par erreur" au cœur de l'extranet de l'Anses, avoir parcouru l'arborescence des répertoires et être remonté jusqu'à la page d'accueil, il avait constaté la présence de contrôles d'accès et la nécessité d'une authentification par identifiant et mot de passe ; qu'il est ainsi démontré qu'il avait conscience de son maintien irrégulier dans le système de traitement automatisé*

de données visité où il a réalisé des opérations de téléchargement de données à l'évidence protégées ; que les investigations ont démontré que ces données avaient été téléchargées avant d'être fixées sur différents supports et diffusées ensuite à des tiers ; qu'il est, en tout état de cause, établi qu'Olivier L. a fait des copies de fichiers informatiques inaccessibles au public à des fins personnelles à l'insu et contre le gré de leur propriétaire ; que la culpabilité d'Olivier L. sera donc retenue des chefs de maintien frauduleux dans un système de traitement automatisé de données et de vol de fichiers informatiques au préjudice de l'Agence Nationale de sécurité sanitaire de l'alimentation, de l'environnement et du travail (Anses) ».

Arrêt complet visualisable ici : https://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=4011

Autre exemple de maintien frauduleux dans un STAD

Cass. Crim., 3 octobre 2007

Une société D. exploite une base de données commerciale dont l'accès est subordonné à un abonnement. Elle reproche à l'un de ses clients, la société P., d'avoir procédé à l'utilisation frauduleuse, de janvier 1998 à juin 2000, d'un logiciel payant.

Selon le gérant de la société P., qui avait précédemment exercé des fonctions commerciales au sein de la société D., lors de l'installation de la base de données, il lui avait été remis un code d'identification permettant aux employés de se connecter gratuitement pendant la période d'essai.

Il ajoutait qu'ultérieurement, ce code n'avait plus à être saisi à chaque connexion. Ce code d'identification provisoire ayant continué de fonctionner, il a permis à la société P. d'accéder à la base de données sans s'acquitter du paiement. Le gérant de la société P. a été renvoyé du chef d'abus de confiance devant le Tribunal correctionnel qui l'a déclaré coupable, en requalifiant les faits, de maintien frauduleux dans un système de traitement automatisé de données.

La Cour de cassation a confirmé ensuite qu'il s'agissait bien d'un maintien frauduleux dans un système de traitement automatisé de données.

Il faut donc pour constituer ce délit, démontrer un accès ou un maintien dans un système automatisé (élément matériel) ainsi qu'une intention frauduleuse (élément moral).

En revanche, serait dépourvue de caractère intentionnel l'action par laquelle un individu accède ou se maintient par hasard ou en toute ignorance dans un système.

Quelques exemples de décisions :

Une décision du Tribunal de Grande instance du 2 juin 2006 a sévèrement condamné un informaticien pour accès frauduleux et entrave au fonctionnement de systèmes informatiques au motif qu'il avait pris le contrôle du serveur d'une société à partir duquel il a lancé des attaques systématiques vers des centaines de sites gouvernementaux pour soit disant « explorer leurs failles ».

394 serveurs gouvernementaux avaient été attaqués ainsi que 63 autres serveurs publics ou privés. L'auteur du piratage a été condamné, à quatre mois de prison avec sursis avec inscription au casier judiciaire, ainsi qu'à indemniser les parties civiles à 1.500 euros chacune.

Concernant le délit d'intrusion dans un STAD, un arrêt de la Cour d'Appel en date du 30 octobre 2002 (plutôt isolé) a abouti à un résultat assez surprenant.

Kitekoa (site internet qui à l'image de Zataz traite de sécurité informatique) a publié un article décrivant un problème sur le site internet www.tati.fr

Il indiquait aux internautes comment en un clic via le navigateur Netscape il était possible de récupérer des milliers de données clients.

Cela a abouti à la condamnation, en première instance, le 13 février 2002, de Kitekoa à une amende de 1000 euros avec sursis.

Le jugement du Tribunal de Grande Instance de Paris qui a précédé celui de la Cour d'Appel avait, en ce sens, estimé que l'existence de failles de sécurité ne constituait :

« *En aucun cas une excuse ou un prétexte pour le prévenu d'accéder de manière consciente et délibérée à des données dont la non-protection pouvait être constitutive d'une infraction pénale* ».

La Cour d'Appel a décidé, le 30 octobre 2002 ; que les intrusions réalisées par le site Kitekoa ne devaient pas être considérées comme une intrusion au sens de la loi notamment en raison du fait :

> ***« Qu'il ne peut être reproché à un internaute d'accéder aux (…) parties de sites qui peuvent être atteintes par la simple utilisation d'un logiciel grand public de navigation, ces parties de site qui ne font par définition l'objet d'aucune protection de la part de l'exploitant du site ou de son prestataire de services, devant être réputées non confidentielles à défaut de toute indication contraire et de tout obstacle à l'accès (…)***
>
> ***Que dès lors les accès dans des parties nominatives du site Tati ne peuvent être qualifiées de frauduleux ».***

Cette décision reste critiquable.

Un accès non autorisé est punissable en tant que tel, même si le site sur lequel l'intrusion a eu lieu était l'objet d'un défaut de sécurisation patent.

Ce défaut de sécurisation qui ne saurait justifier une intrusion dans un réseau n'empêche pas que le titulaire du site soit sanctionné pénalement si une loi imposait qu'un niveau de protection particulier soit mis en place sur le site notamment concernant les données personnelles qu'il contient.

La décision Kitekoa était en réalité guidée par l'équité.

L'article 226-17 du Code pénal réprime, en effet :

> *« Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en oeuvre les mesures prescrites à l'article 34 de la loi n° 78-17 du 6 janvier 1978, à savoir les précautions utiles pour préserver la sécurité de ces informations et notamment d'empêcher qu'elles ne soient communiquées à des tiers non autorisées, est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende ».*

En l'espèce la personne qui s'était introduite sur le site tati.fr avait immédiatement averti les administrateurs du site sans chercher à tirer avantage de la faille qu'elle avait trouvée.

Finalement poursuivie par Tati.fr pour intrusion dans un STAD, il convenait de trouver une solution qui ne viendrait pas sanctionner une situation qui ne relevait pas d'une volonté de nuire.

2) L'interception illégale de données

L'interception illégale se définit comme « *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* ».

Cette infraction est punie d'un an d'emprisonnement et de 45000 euros d'amende par l'article 226-15 du Code pénal. « *Est puni des mêmes peines le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie électronique ou de procéder à l'installation d'appareils conçus pour réaliser de telles interceptions* » précise ce même article.

3) L'entrave au fonctionnement d'un système automatisé de données

L'article 323-2 du Code pénal incrimine le fait de fausser ou d'entraver le fonctionnement du système automatisé de données. Cela est passible de cinq ans d'emprisonnement et de 75 000 euros d'amende[3].

---

[3] Modifié par LOI n°2012-410 du 27 mars 2012 - art. 9
Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75000 euros d'amende.

Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 100 000 euros d'amende.

Peu importe qu'il y ait eu accès – autorisé ou non – au système informatique de la victime, il s'agit ici de réprimer des dégâts causés volontairement aux données et au système, notamment, par exemple, par l'introduction d'un virus.

L'envoi massif de courriels non sollicités (ou spamming) est un autre exemple d'entrave au système (CA Paris, 18 déc. 2001, D. 2002, p. 940).

En revanche, pour que l'infraction soit constituée, il faut que le fonctionnement du système soit faussé ou entravé, c'est-à-dire qu'il soit affecté de manière préjudiciable.

4) La modification frauduleuse de données

L'article 323-3 du Code pénal vise la modification frauduleuse de données.

Il sanctionne l'introduction, la suppression ou la modification frauduleuse de données de cinq ans d'emprisonnement et de 75 000 euros d'amende. À titre d'exemple, le groupe de hackers qui avait profité d'une faille pour s'introduire sur le site Internet de la mission interministérielle de lutte contre la drogue a également été condamné pour modification frauduleuse de données.

Ils avaient, en effet, remplacé un texte qui figurait sur le site, par des propos incitant à la consommation de cannabis (CA Paris, 28 janv. 2010)

Cette pratique est également appelée défacement ou altération quand il s'agit de la page d'accueil d'un site web. Un défacement, défaçage ou défiguration (defacing en anglais) est un anglicisme désignant la modification non sollicitée de la présentation d'un site web, à la suite du piratage de ce site. Il s'agit donc d'une forme de détournement de site Web par un hacker.

En France par exemple, les sites de l'Élysée et Hadopi.fr ont ainsi été attaqués par Anonymous suite à la fermeture de Megaupload.

5) La répression des créateurs, importateurs et diffuseurs de virus et autres logiciels malveillants

L'article 323-3-1 du Code pénal vise quant à lui les moyens qui permettent ces attaques et punit des mêmes peines l'importation, la détention, l'offre, la cession et la mise à disposition de ces moyens techniques, matériels ou logiciels.
Sont ainsi directement visés les créateurs de virus.

Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 100 000 € d'amende.

Cet article dispose que : **«** *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* ».

6) La tentative des délits prévus par les articles 323-1 à 323-3-1 est punie des mêmes peines.

En matière de fraude informatique, la tentative est réprimée de la même manière que le délit que l'on souhaitait parvenir à commettre.

Cela signifie, par exemple, qu'il est inutile de soutenir en cas de tentative avérée d'entrave au fonctionnement dans un STAD, qui s'est finalement révélée infructueuse, qu'on ne risque aucune amende ni aucune peine d'emprisonnement au motif que le résultat n'a pas été atteint.

De la même façon, la tentative d'intrusion qui n'a pas abouti pourra être sanctionnée par la même peine que l'intrusion stricto sensu.

7) Association de malfaiteurs en vue d'une intrusion dans un STAD

L'article 323-4 du Code pénal permet de réprimer les associations de malfaiteurs, dès leurs premiers efforts accomplis en vue de l'intrusion.

« *La participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions prévues par les articles 323-1 à 323-3-1 est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée* ».

Ex : Anonymous, Wikileaks

8) Le recel d'informations obtenues suite à une intrusion dans un STAD

Le recel d'informations obtenues à la suite d'une intrusion frauduleuse dans un système de traitement automatisé de données est puni par l'article 321-1 du Code pénal de cinq ans d'emprisonnement et de 375 000 euros d'amende.

Jurisprudence :

Le 10 novembre 2011, le Tribunal correctionnel de Nanterre a lourdement condamné le piratage du système d'information de l'association Greenpeace perpétré par une société d'intelligence économique au bénéfice de la société EDF.

Le Tribunal de Nanterre a prononcé des sanctions d'emprisonnement et d'amende à l'encontre du Hacker (2 ans d'emprisonnement dont 13 mois avec sursis et 4.000 euros d'amende) de la société d'intelligence économique et de deux des salariés d'EDF.

Une condamnation à un million et demi d'euros d'amende a été prononcée à l'encontre d'EDF pour recel et complicité d'intrusion dans un STAD. Les magistrats ont considéré que les salariés responsables de la sécurité d'EDF n'avaient pas agi pour leur compte personnel mais dans l'intérêt exclusif d'EDF qui a pu bénéficier des informations sur un CD-ROM détenu dans ses locaux.

Les personnes morales (entreprises / associations) s'exposent, par principe, à une amende 5 fois supérieure à celle d'une personne physique (individu, particulier).

Cela est prévu à l'article 131-38 du Code pénal qui dispose que :

« Le taux maximum de l'amende applicable aux personnes morales est égal au quintuple de celui prévu pour les personnes physiques par la loi qui réprime l'infraction ».

Ainsi, si la personne condamnée est une personne morale (entreprise, association), elle peut être condamnée à une amende d'un montant 5 fois supérieur à l'amende prévue par la loi. En l'espèce, 375 000 X 5 = 1 875 000 euros.

9) Usurpation d'identité

La loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure (dite LOPPSI 2) a créé un nouveau délit d'utilisation frauduleuse de l'identité ou de données à caractère personnel d'un tiers sur un réseau de communications électroniques, comblant ainsi un vide juridique.

Ce nouveau délit s'applique à l'usurpation de l'identité des personnes morales et physiques qui sont très souvent victimes de ce type de comportement délictueux (notamment via le phishing).

Cette loi crée ainsi un nouvel article 226-4-1 du Code pénal aux termes duquel :

> *« Le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération ou ses intérêts, est puni d'un an d'emprisonnement et de 15 000 euros d'amende. Cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne ».*

L'hameconnage et le phishing peuvent être punis sur la base de cet article.

L'apport de la LOOPSI 2

La LOPPSI 2 représente, à ce titre, une avancée considérable dans la mesure où elle permet aux forces de l'ordre de recourir à la captation à distance de données informatiques dans les affaires de criminalité organisée.

C**ette nouvelle procédure particulièrement intrusive est fort heureusement très encadrée et limitée au champ spécifique de la criminalité organisée.**

Toutes ces évolutions devraient permettre aux entreprises – comme aux personnes physiques d'ailleurs – d'être de mieux en mieux protégées contre la cybercriminalité.