L'INTRUSION ET LES ATTEINTES AUX SYSTEMES INFORMATIQUES SANCTIONNEES PAR LE DROIT PENAL

publié le **10/09/2010**, vu **30406 fois**, Auteur : Anthony BEM

Afin de protéger les systèmes informatiques contre les atteintes dont ils peuvent faire l'objet, la loi n°88-19 dite Godfrain du 5 janvier 1988, relative à la fraude informatique, a établi une série de sanctions pour quatre catégories de fautes distinctes : - l'intrusion - le maintien frauduleux ou irrégulier - l'entrave au fonctionnement - l'introduction frauduleuse de données

Cette loi a été reprise dans le nouveau code pénal entré en vigueur en 1994 qui a codifié ces fautes au sein des articles 323-1 et suivants.

Mais de quoi s'agit-il concrètement ?

Lors de l'élaboration du nouveau code pénal, le Sénat avait proposé de définir le système de traitement automatisé de données comme « *tout ensemble composé d'une ou plusieurs unités de traitement, de mémoire, de logiciel, de données, d'organes d'entrées-sorties et de liaisons, qui concourent à un résultat déterminé, cet ensemble étant protégé par des dispositifs de sécurité* ».

Cependant, le législateur n'a finalement retenu aucune définition.

Il a été jugé que constituent un « système de traitement automatisé de données » notamment :

- un disque dur (Cour d'appel de Douai, 7 oct. 1992)
- un radiotéléphone (Cour d'appel de Paris, 18 nov. 1992)
- le réseau Carte bancaire (Trib. cor. Paris, 25 fev. 2000)

L'article 323-1 al. 1er du code pénal défini l'intrusion comme le *"fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données."*

Si l'incrimination vise tous les modes de pénétration irréguliers d'un système de traitement automatisé de données, l'accès ne tombe sous le coup de la loi pénale que s'il est le fait d'une personne qui n'a pas le droit d'accéder au système ou n'a pas le droit d'y accéder de la façon dont elle y a accédé.

De plus, la loi réprime non seulement l'intrusion mais aussi le maintien frauduleux ou irrégulier dans un système de traitement automatisé de données de la part de celui qui est entré par inadvertance, ou de la part de celui qui, ayant régulièrement pénétré, se serait maintenu frauduleusement.

L'intrusion ou le maintien dans un système informatique est puni de deux ans d'emprisonnementet 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.

L’article 323-2 du même code réprime l’entrave au fonctionnement du système informatique en ce qu’il dispose que : « 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.

L'entrave du fonctionnement d'un système de traitement automatisé de données correspond parfois à une impossibilité totale d'utiliser le système, par exemple le blocage d'un code d'accès ou la paralysie de son fonctionnement.

Elle peut également consister en une simple diminution de la capacité de traitement.

Le trouble peut être permanent, par exemple lorsque le système est infesté d'un virus, il peut également se reproduire à échéance régulière, notamment lorsqu'une « bombe logique » a été insérée pour paralyser régulièrement le fonctionnement du système.

Enfin, l’article 323-3 du code pénal sanctionne l’introduction frauduleuse de données en ce qu’il dispose que : *"le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75000 euros d'amende."*

S’agissant des sanctions, le législateur a imaginé des peines complémentaires pour les personnes physiques, à savoir :

1° L'interdiction, pour une durée de cinq ans au plus, des droits civiques, civils et de famille, suivant les modalités de l'article 131-26 ;

2° L'interdiction, pour une durée de cinq ans au plus, d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale dans l'exercice de laquelle ou à l'occasion de laquelle l'infraction a été commise ;

3° La confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit, à l'exception des objets susceptibles de restitution ;

4° La fermeture, pour une durée de cinq ans au plus, des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ;

5° L'exclusion, pour une durée de cinq ans au plus, des marchés publics ;

6° L'interdiction, pour une durée de cinq ans au plus, d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés ;

7° L'affichage ou la diffusion de la décision prononcée dans les conditions prévues par l'article 131-35.

S’agissant de la compétence des juges français il est important de rappeler qu’à chaque fois où le dommage est survenu au sein d’un système informatique d’une société domiciliée en France ou que l’une des infractions précitées est commise sur le territoire national, les juridictions françaises sont compétentes pour en connaître.

Afin de se prémunir contre les conséquences de ce type d’événement, il convient d’une part d’insérer dans tous les contrats techniques une clause concernant la sécurité du contenu du système en cause notamment en déterminant les conditions d’accès au serveur en tant que matériel informatique ou en prévoyant les technologies disponibles afin d’y remédier.

Enfin, outre une action sur le plan pénal, il est possible de souscrire une assurance contre le risque d’attaque informatique afin d’obtenir le dédommagement des préjudices subis.

Je suis à votre disposition pour toute information ou action.

PS : Pour une recherche facile et rapide des articles rédigés sur ces thèmes, vous pouvez taper vos "mots clés" dans la barre de recherche du blog en haut à droite, au dessus de la photographie.

Anthony Bem
Avocat à la Cour
27 bd Malesherbes - 75008 Paris
Tel : 01 40 26 25 01

Email : abem@cabinetbem.com

www.cabinetbem.com