Droit du numérique

Support de cours : « Intrusion frauduleuse dans un Système de Traitement Automatisé de Données »

sylvie.bourlier@free.fr

Intrusion frauduleuse dans un Système de traitement Automatisé de Données

$1 Responsabilité pénale

A/ Intrusion sans dommage

La cybercriminalité est réprimée sur le plan pénal par le biais de l'accès ou du maintien frauduleux dans un système de traitement automatisé de données et ceci même en l'absence de dommage.

Article 323-1 Code pénal
Version en vigueur depuis le 26 janvier 2023
Modifié par LOI n°2023-22 du 24 janvier 2023 - art. 6

« Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de trois ans d'emprisonnement et de 100 000 € d'amende. »
Un site internet est considéré comme un STAD.

Pour qu'il y ait infraction en droit pénal, il faut réunir trois éléments :

- Elément légal : article 323-1 Code pénal
- Elément matériel de l'infraction : l'accès ou le maintien
- Elément moral : le caractère frauduleux

1) Accès frauduleux

La Cour d'appel de Paris a considéré dans un arrêt du 5 avril 1994 que " *l'accès frauduleux, au sens de la loi, vise tous les modes de pénétration irréguliers d'un système de traitement automatisé de données, que l'accédant travaille déjà sur la même machine mais à un autre système, qu'il procède à distance ou qu'il se branche sur une ligne de communication ".*

Qu'en est-il lorsque le système comporte des failles de sécurité ? La Cour d'appel de Paris, dans un arrêt en date du 30 octobre 2002, a jugé que la possibilité d'accéder à des données stockées sur un site avec un simple navigateur, en présence de nombreuses failles de sécurité, n'est pas répréhensible.
En effet, dans ce cas, l'intension frauduleuse, la conscience de faire quelque chose d'illégal ne peut être prouvée.

Il est à noter que dans le cas de failles de sécurité le responsable du traitement s'expose à une sanction.

Article 226-17 alinéa 1 du Code pénal
Version en vigueur depuis le 01 juin 2019
Modifié par Ordonnance n°2018-1125 du 12 décembre 2018 - art. 13

« Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites aux articles 24,25,30 et 32 du règlement (UE) 2016/679 du 27 avril 2016 précité ou au 6° de l'article 4 et aux articles 99 à 101 de la loi n° 78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende. »

2) Le maintien frauduleux

La loi incrimine également le maintien frauduleux ou irrégulier dans un système de traitement automatisé de données de la part de celui qui y est entré par inadvertance ou de la part de celui qui, y ayant régulièrement pénétré, se serait maintenu frauduleusement (Cour d'appel de Paris, jugement du 5 avril 1994 précité).
" frauduleusement " fait référence à la conscience chez le délinquant que l'accès ou le maintien ne lui était pas autorisé.

Dans ce cas, d'éventuelles failles de sécurité n'exonèrent pas l'auteur du maintien de sa responsabilité.

B/ Les intrusions avec dommages

Lorsque l'intrusion s'accompagne de dommages ou que l'infraction à été commise à l'encontre d'un système automatisé de traitement de données, les peines sont renforcées.
Ainsi**, l'article 323-1 alinéas 2 et 3** :
« 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 cinq ans d'emprisonnement et de 150 000 € 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 sept ans d'emprisonnement et à 300 000 € d'amende. »
Il s'agit là d'une altération involontaire car il est écrit « Lorsqu'il en est résulté »

L'article 323-2 du Code pénal définit, quant à lui, l'entrave volontaire au système comme "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 150 000 euros d'amende. »
Si STAD de données à caractère personnel mis en œuvre par l'Etat : sept ans, 300 000 euros.
Cette infraction vise, notamment, l'introduction des programmes susceptibles d'entraîner une perturbation au système, tels que des virus.

L'article 323-3 du Code pénal sanctionne, pour sa part, « Le fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 150 000 € d'amende. »

Si STAD de données à caractère personnel mis en œuvre par l'Etat : sept ans, 300 000 euros.

Les applications illicites visées par cet article vont de la réduction du prix des marchandises sur un site de commerce électronique, la modification ou la suppression du contenu des bases de données à la modification du statut fiscal de l'entreprise.

$2 La responsabilité civile

La cybercriminalité peut également entraîner une action en responsabilité civile contractuelle ou délictuelle selon que l'auteur du dommage est, ou non lié, par un contrat avec la personne en demandant réparation.

1) La responsabilité civile délictuelle

Le droit commun de la responsabilité civile délictuelle est fondé sur la notion de la faute au sens de l'article 1240 du Code civil.

Article 1240

Version en vigueur depuis le 01 octobre 2016

« Tout fait quelconque de l'homme, qui cause à autrui un dommage, oblige celui par la faute duquel il est arrivé à le réparer. »

Trois conditions sont nécessaires pour faire jouer cette responsabilité : une faute, un dommage et un lien de causalité entre les deux.

La faute consiste en l'intrusion frauduleuse dans un système informatique.

Le dommage est la perte et/ou l'altération des informations contenues dans le site ou bien encore la communication des données personnelles présentes sur le site à des tiers.

Le lien de causalité entre la faute et le dommage doit être clairement établi.

2) La responsabilité civile contractuelle.

Selon les clauses du contrat liant le propriétaire du site à son hébergeur, la responsabilité contractuelle de ce dernier pourra être engagée.

Il conviendra d'étudier les clauses contenues dans le contrat d'hébergement concernant notamment la sécurité du site et la mise en place de systèmes informatiques de protection contre toute forme d'intrusion.