Loi : Intrusion dans un système informatique (hacking)

publié le **01/05/2009**, vu **1004469 fois**, Auteur : Murielle Cahen

Il existe différents types de pirates informatiques : du hacker classique, qui 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, au cracher (casseur), appellation qui désigne le pirate qui détruit dans un but précis ou pour le plaisir. Les « crachers » sont par définition dangereux puisque animés d'une intention de nuire évidente (vol etc.), tandis que les autres peuvent être simplement poussés par la curiosité ou la volonté d'enquêter dans le but d'informer les détenteurs de systèmes de traitement automatisé de données (STAD) des failles dans leur dispositif de sécurité. Or, aux yeux de la loi, chacun d''entre eux peut être poursuivi au regard des dispositions du Code pénal en matière de fraude informatique.

Il existe différents types de pirates informatiques : du *hacker* classique, qui 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, au *cracher* (casseur), appellation qui désigne le pirate qui détruit dans un but précis ou pour le plaisir. Les « crachers » sont par définition dangereux puisque animés d'une intention de nuire évidente (vol etc.), tandis que les autres peuvent être simplement poussés par la curiosité ou la volonté d'enquêter dans le but d'informer les détenteurs de systèmes de traitement automatisé de données (STAD) des failles dans leur dispositif de sécurité. Or, aux yeux de la loi, chacun d''entre eux peut être poursuivi au regard des dispositions du Code pénal en matière de fraude informatique.

La loi dite « Godfrain » du 5 Janvier 1988 (n° 88-19) a introduit dans le code pénal l'article 462-2 a crée le délit d'intrusion dans un système informatique.

La loi « pour la confiance dans l'économie numérique » du 21 juin 2004 (n° 2004-575) a déplacé et modifié ce texte, désormais présent à l'article 323-1 du code pénal, lequel dispose que « *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.* »

Un système de traitement automatique de données c'est, selon les magistrats, par exemple un réseau, réseau France Telecom, réseau Carte Bancaire (Tribunal correctionnel de Paris, 25 février 2000) ; un disque dur (Cour d'appel de Douai, 7 octobre 1992) ; un radiotéléphone (Cour d'appel de Paris, 18 novembre 1992). En tout cas, tous les équipements (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.

Ainsi, toute intrusion ou maintien frauduleux dans un STAD est pénalement répréhensible, ce qui recouvre un grand nombre d'hypothèses.

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.* »

Toutefois, dans un arrêt du 4 décembre 1992, la Cour d''appel de Paris a écarté les délits d''accès et de maintien dans un système de traitement automatisé de données informatiques en constatant que l''appropriation d''un code d''accès avait pu être le résultat d''une erreur de manipulation sur les fichiers, cette circonstance excluant le caractère intentionnel exigé par la loi. Ainsi, une intrusion accidentelle ne peut être incriminée, encore faut il ne pas se maintenir dans le STAD accidentellement atteint.

De plus, dans un arrêt du 3 octobre 2007, la Cour de Cassation estime que « *Doit être censuré l''arrêt qui relaxe un prévenu du chef de maintien frauduleux dans un système de traitement automatisé de données alors qu''il relève que celui-ci, quand bien même il y aurait accédé régulièrement, a utilisé pendant plus de deux ans, et avec un code qui ne lui avait été remis que pour une période d''essai, une base de données qui n''était accessible qu''aux personnes autorisées*. »

En clair, relèvent de la qualification pénale toutes les intrusions intentionnelles (non accidentelles) irrégulières, mais aussi régulières si elles dépassent l'autorisation donnée. Qu'est ce qu'une intrusion irrégulière ? Une intrusion irrégulière recouvre une intrusion non autorisée par le maître du système.

La question qui vient alors à se poser est la suivante : l'infraction pénale est elle constituée par un accès à un STAD non protégé ? La présence d'un dispositif de sécurité est elle une condition de l'incrimination pénale ?

Le 30 octobre 2002, dans une affaire célèbre opposant la société TATI à un journaliste, spécialisé en informatique, administrateur du site internet KITETOA.COM, la Cour d''appel de Paris est venue nuancer sa jurisprudence antérieure. Sur appel à l''encontre du jugement de condamnation du Tribunal de grande instance de Paris en date du 13 février 2002, le prévenu a été relaxé. La Cour a considéré qu''on ne pouvait pas reprocher à un internaute d''accéder ou de se maintenir dans les parties d''un site accessible par la simple utilisation d''un logiciel de navigation, et que « *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 (...). La détermination du caractère confidentiel et des mesures nécessaires à l''indication et à la protection de cette confidentialité relevant de l''initiative de l''exploitant du site ou de son mandataire.* »

En un mot, le problème juridique soulevé par le juge repose sur le fait que la partie plaignante a manqué aux obligations légales de protections de données.

Par extension, on peut dire que cette affaire met en l''application l''adage nemo pluri juris nullis turpitudis (nul ne peut se prévaloir de sa propre turpitude). Cette jurisprudence conduit à exiger la mise en place d''une protection adaptée du système ou, lorsqu''il s''agit d''un serveur Internet, de codes et mots de passe en restreignant utilement l''accès. En l''absence de toute mesure de protection, l''accès ou le maintien pourrait ne pas être considéré comme «frauduleux« au sens de la loi. Mais quid des abus que les esprits malveillants peuvent tirer de ce manquement aux

obligations de protection ?

Rappelons que l''article 29 de la loi du 6 janvier 1978 dite «Informatique et Libertés » dispose que : « Toute personne ordonnant ou effectuant un traitement d''informations nominatives s''engage de ce fait, vis-à-vis des personnes concernées, à prendre toutes précautions utiles afin de préserver la sécurité des informations et notamment d''empêcher qu''elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés. » Il s''agit d''une «obligation de sécurité des données personnelles«, dont le non-respect est sanctionné par l''article 226-17 de nouveau Code pénal : « Le fait de procéder ou de faire procéder à un traitement automatisé d''informations nominatives sans prendre toutes les précautions utiles pour préserver la sécurité de ces informations et notamment empêcher qu''elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés est puni de cinq ans d''emprisonnement et de 2.000.000 francs d''amende. »

L’absence de dispositif de sécurité est elle un obstacle à l’infraction pénale d’intrusion ou maintien frauduleux dans un STAD ? La réponse qui s’impose est négative. En effet, si le maître d’un STAD ne remplit pas ses obligations légales de sécurisation des données, cela n’autorise cependant pas d’autres personnes à s’introduire dans le système et/ou s’y maintenir, même en l’absence d’une volonté de nuire. **L’affaire de 2002 (Kitetoa/Tati), qui n’a pas trouvé d’écho en jurisprudence semble plutôt être une décision isolée motivée par l’équité.**

Dans une décision du 5 avril 1994, la Cour d''appel de Paris avait précisé que « *pour être punissable, cet accès ou ce maintien doit être fait sans droit et en pleine connaissance de cause, étant précisé à cet égard qu''il n''est pas nécessaire pour que l''infraction existe que l''accès soit limité par un dispositif de protection*. » La Cour a encore précisé qu''il suffit, pour que l''accès ou le maintien soit «punissable » que «*le maître du système ait manifesté l''intention d''en restreindre l''accès aux seules personnes autorisées.* »

Il semble donc prudent d’affirmer que malgré l’absence de dispositif de sécurité, l’intrusion dans un STAD constitue une infraction pénale. L’implication pratique de ces données jurisprudentielles est aujourd’hui conséquente, notamment avec l’apparition de la technologie Wi-Fi. En effet, un réseau Wi-Fi semble répondre à la qualification de STAD et si l’intrusion à un tel réseau protégé ne pose pas de problème majeur, la connexion à un réseau Wi-Fi non protégé pose quelques interrogations. En l’absence de jurisprudence sur ce point, la conclusion logique serait la suivante : sauf à ce que le propriétaire du réseau exprime clairement sa volonté d’ouvrir sa connexion au public (hotspots Wi-Fi etc.), se connecter à un réseau non protégé pourrait être un fait constitutif de l’infraction pénale prévue par l’article 323-1 du code pénal.