

Contribution de la Brigade d'Enquêtes sur les Fraudes aux Technologies de l'Information (BEFTI) au forum « Données de connexion »

Présentation de la B.E.F.T.I.

La B.E.F.T.I., service de la Direction Régionale de la Police Judiciaire de Paris créé en Février 1994, a pour mission essentielle de lutter contre les atteintes aux systèmes de traitement automatisés d'informations, qu'il s'agisse des réseaux informatiques ou télématiques, ou des systèmes de télécommunications (GSM, autocommutateurs d'entreprises...).

Son domaine d'action ne se limite cependant pas aux intrusions dans les systèmes d'informations, mais vise également la lutte contre la contrefaçon sur supports numériques, la captation frauduleuse de médias télévisuels cryptés, ainsi que des incriminations traditionnelles utilisant les nouvelles technologies comme support de commission. Il s'agit alors de l'escroquerie (y compris dans le milieu de la télématique), de détournements de fonds, d'abus de confiance, d'atteintes aux biens (recel de vol), d'atteintes à la personne (injures, diffamation) ou prévues par la loi du 29 juillet 1881 (Loi sur la liberté de la presse) perpétrées sur les réseaux.

La B.E.F.T.I. joue également un rôle important dans l'assistance technique sollicitée par les autres services de police lorsque ces derniers sont confrontés à la recherche de la preuve sur supports numériques découverts dans leurs propres enquêtes (disques durs, disquettes, CD Rom...).

Dans ce contexte, la B.E.F.T.I. constate une augmentation régulière de l'utilisation du média Internet dans la commission de nombreux délits avec comme corollaire une augmentation très inquiétante d'enquêtes non résolues. Ce constat s'expliquant essentiellement par un archivage des données techniques insuffisant dans le temps.

Intérêt de l'archivage des données techniques

Il apparaît plus opportun, dans le cadre du Forum des Droits de l'Internet, de développer pourquoi un acte malveillant commis sur la toile conserve aujourd'hui toutes les chances de ne pas être élucidé, que de décrire ici dans le détail quelles sont les données techniques qui doivent ou non être stockées.

Dans un second temps, il serait souhaitable que nous ayons une approche plus technique pour confronter ainsi les expériences pratiques. Cela devrait permettre d'avoir collectivement une vision plus objective et moins passionnée du sujet. Cette approche constructive pourrait se faire à l'occasion de rencontres entre les diverses parties prenantes où les différentes composantes du Net (Web, Mail, Forums, Chats) devront être étudiées.

Ce travail d'analyse devra en outre faire la distinction entre certaines catégories d'incriminations. De nombreux exemples concrets pourront alors être exposés.

Plusieurs éléments militent donc en faveur d'un archivage des informations indispensables à la traçabilité des infractions commises sur les réseaux.

Sur le plan interne, tout d'abord, le délai séparant la commission de l'infraction et le moment où la victime constate la réalité des faits peut atteindre plusieurs semaines. Le cas du particulier doit ici être distingué du cas de l'entreprise :

- le particulier disposant d'un PC relié à Internet s'apercevra rapidement, notamment en cas d'attaque virale, d'une intrusion sur son ordinateur. Ce même particulier procédant à un achat en ligne ne constatera l'utilisation frauduleuse de ses références bancaires que plusieurs semaines après le débit de l'opération litigieuse si l'on veut bien considérer l'addition du délai d'envoi des relevés d'opérations bancaires qui pour certains établissements peut atteindre deux mois, au délai de réactivité desdits établissements vis à vis d'opérations effectuées le plus souvent sur des sites résidants à l'étranger.

- concernant les entreprises, les intrusions commises dans leurs systèmes d'informations demeurent ignorées dans 80% des cas (idem aux U.S.A.) contribuant ainsi, en partie, à générer un chiffre noir qui en matière de criminalité informatique approche les 90%. La révélation d'un piratage intervient le plus souvent après un délai supérieur au délai aujourd'hui librement pratiqué par les professionnels de l'internet.

Sur le plan international cette fois, le temps nécessaire à la transmission d'une commission rogatoire internationale d'un pays requérant vers un pays destinataire peut demander plusieurs mois.

Récemment, la B.E.F.T.I. a été dans l'impossibilité de répondre aux demandes de la justice américaine lorsqu'en septembre 2000, celle-ci a sollicité des investigations auprès de FAI français suite aux actes de piratages qu'ont connus en février et mars 2000 les plus importants sites de commerce en ligne américains.

Pour démontrer également quels peuvent être les obstacles techniques rencontrés dans la résolution d'une enquête, certains FAI ont recours à des serveurs intermédiaires de type « proxy » installés pour améliorer la qualité d'accès aux informations disponibles sur le WEB. Ces matériels ne fournissent, à ce jour, aucune donnée technique exploitable au delà de quelques heures (!) annulant cette fois-ci toute possibilité d'identification.

Résultat : 25% des plaintes (toutes incriminations confondues) traitées par la B.E.F.T.I. n'aboutissent pas du seul fait du non stockage des données techniques.

Il devient alors difficile de faire comprendre cet état de fait aux victimes qui voient se renforcer leur sentiment d'insécurité vis à vis de la toile alors que le sentiment d'impunité de ceux qui utilisent le réseau à des fins malveillantes risque de s'amplifier.

Eu égard à ces éléments sommairement développés, le délai d'un an semble donc, contrairement à la vision de la C.N.I.L. sur ce sujet, des plus raisonnable. La comparaison qui peut être faite avec les autres pays européens concernant ce délicat problème du délai d'archivage des données de connexion, n'a réellement d'intérêt qu'à partir du moment où nous comparons également l'état des faits constatés en matières d'infractions liées aux NTIC pour chaque pays considéré.

Si l'archivage de ces informations représente évidemment un coût non négligeable pour les professionnels de l'Internet, les solutions techniques existent déjà en partie et sont utilisées par certains d'entre eux qui archivent au delà du délai de trois mois actuellement pratiqué.

L'archivage des données techniques ne permettra pas de contrer toutes les difficultés qui empêchent actuellement d'avoir une traçabilité efficace sur le réseau. Les serveurs permettant de rester anonyme, la mise en ligne d'informations et de solutions logicielles permettant de commettre des intrusions, de contourner des sécurités, de générer des

numéros de cartes bleues à l'aide d'algorithmes mathématiques cohérents, continuent, faute de correspondre à des incriminations autonomes, d'être largement utilisés.

La solution est nécessairement globale car elle implique une plus grande coopération entre les systèmes judiciaires de tous les pays et une harmonisation des différentes législations. Mais il n'est pas vain pour autant de réfléchir, d'essayer d'anticiper sur les risques qui consistent à laisser se développer sur le Net non pas un espace de liberté, mais un espace où aucune règle reconnue par tous ne serait en mesure d'instaurer la confiance.

Il importe donc de développer cette confiance dans le réseau en améliorant la sécurité des informations qui peuvent y être consultées et échangées. De cela dépendra en grande partie le démarrage de cette « Net économie » qui reste aujourd'hui quelque peu balbutiante.