Les détectives privés enquêtent en infiltration et sous pseudonyme- Cybercrime, Bitcoin

Fiche pratique publié le **30/10/2018**, vu **2662 fois**, Auteur : Alain STEVENS

La résolution des enquêtes dans le domaine de la cybercriminalité ne peut pas aboutir uniquement avec les réquisitions judiciaires. Les détectives privés et les consultants en cybercriminalité peuvent obtenir des informations probantes en menant des enquêtes numériques en infiltration.

Déposer plainte ou attendre les résultats d'une levée d'anonymat, ce n'est pas suffisant pour faire valoir ses droits quand on est victime du cybercrime.

Face au nombre croissant des contentieux en cybercriminalité, avec un préjudice de plus de 6 milliards d'euros, les détectives privés spécialisés dans les enquêtes numériques sont un recours très utile quand survient un litige.

Les victimes de la cybercriminalité ont de plus en plus de difficultés à défendre leurs intérêts devant les tribunaux, et le RGPD complique beaucoup les investigations privées et publiques. Des investigations privées sous couverture et en infiltration peuvent permettre de connaître à l'avance des résultats de réquisitions judiciaires (1).

Mais de plus en plus de plaintes ne sont pas instruites, faute de preuves et d'indices exploitables. Les délais imposés par l'administration et la machine judiciaire laissent se prolonger des situations à risques, avec des sites frauduleux qui continuent à faire de nombreuses victimes alors même qu'ils sont signalés par les autorités.

D'ailleurs, il faut observer qu'un simple signalement aux autorités peut être suffisant pour qu'une enquête soit diligentée. En Belgique, plus de 6 plaintes sur 10, dans des affaires de fraudes en ligne, sont classées sans suite, en particulier parce que les identifications sont impossibles ou très compliquées.

L'exemple typique est celui des escroqueries au Bitcoin et aux cryptomonnaies en général, avec des sites signalés sur la liste de l'Autorité des Marchés Financiers (2), et malgré tout plus que jamais actifs.

Comment préserver les preuves numériques ?

Entre le moment où la victime se rend compte de la fraude, et la prise en charge de l'instruction, il peut s'écouler plusieurs semaines pendant lesquelles les cyberdélinquants auront tout le temps de dissimuler leurs traces.

- fermeture des comptes mails impliqués

- réaffectation des numéros de mobile
- suppression des sites incriminés
- changement d'hébergeur

Dans certains cas, les victimes vont d'adresser à des avocats spécialisés en cybercriminalité, qui mettront en place des procédures pour obtenir des données d'identification auprès des hébergeurs, ou des fournisseurs de services, comme Google (pour Gmail et Youtube), Twitter ou Facebook.

La levée de l'anonymat d'une personne à l'origine d'actions malveillantes nécessite en effet une demande auprès d'un juge.

Il va falloir, là aussi, attendre plusieurs semaines pour obtenir des informations. Un délai supplémentaire qui favorisera l'effacement de traces numériques qui pourraient conduire à des preuves.

L'analyse de ces données ne permettra pas, de façon systématique, de connaître l'identité des personnes ayant participé au délit. Par exemple, une requête adressée auprès deTwitter aboutira à la communication d'une adresse IP anonyme, c'est-à-dire attribuée par un logiciel qui anonymise sa connexion.

Ensuite, on obtiendra une adresse email associée au compte, mais il faudra, une fois de plus, demander une nouvelle réquisition.

La réquisition, en tant que telle, peut donc ne constituer qu'un des éléments qui va participer à la manifestation de la vérité.

Mais le consultant en cybercriminalité, qui sera sollicité en parallèle, pour mener des investigations numériques, ou bien le détective privé disposant de compétences en sécurité informatique et réseaux, pourra de son côté découvrir des informations très utiles, surtout pour faire des recoupements.

Des réquisitions peuvent s'accompagner d'investigations privées

Il est fréquent qu'une réquisition mentionne une IP de proxy. Une adresse IP de proxy n'est pas identifiable en tant que telle. Mais il faut quand même observer que des recoupements sont possibles, par exemple avec des connexions d'autres pseudos, ou d'autres profils impliqués dans les enquêtes.

Ces techniques d'infiltration numérique permettent en effet de connaître à l'avance certains résultats de ces réquisitions. C'est un élément très intéressant, parce qu'elles permettent de gagner du temps, d'économiser le coût de certaines procédures inutiles, et de mieux cibler les actions des avocats.

Prenons l'exemple de propos diffamatoires, publiés depuis un blog anonyme, un compte Twitter, des vidéos Youtube, et des courriers électroniques.

Le premier réflexe sera de demander des réquisitions pour toutes les pistes, sans oublier, au préalable, de faire constater par huissier toutes les contributions publiques ou privés à l'origine de la diffamation.

Les enquêtes privés renforcent l'efficacité des réquisitions

Mais que faire si toutes ces réquisitions se soldent par des résultats inexploitables ?

Le travail préalable du consultant en cybercriminalité, qui pourra d'ailleurs collaborer avec des détectives privés, consistera à mettre en place des "pièges numériques", des plateformes informatiques dédiées à l'investigation.

S'agit-il pour autant d'actions illicites ou de piratage ?

Le professionnel des enquêtes numériques ne prendra pas le risque de commettre des actions illicites qui pourrait faire annuler les procédures en cours ou de se retourner contre lui.

Au contraire, avec ses investigations sous couverture, sa connaissance des réseaux, il va pouvoir être en mesure d'identifier des données utiles à l'enquête future, parce qu'il saura, par exemple, qu'un délinquant s'est connecté depuis son domicile à telle date et telle heure, ou bien que tel faux profil aura été créé avec une adresse mail personnalisée, composée de son identité réelle et du nom de son fournisseur d'accès.

Il va donc communiquer ces informations à l'avocat, qui va pouvoir officialiser ces informations "en zone grise", dont on sait déjà qu'elles vont permettre de résoudre de façon certaine l'enquête en cours.

Faut-il encadrer ces procédures ?

Elles ne sont pas engagées par des membres de l'administration, mais par des professionnels indépendants, et elles restent conformes à la législation. Ce ne sont pas des techniques d'enquête intrusive, comme il en existe dans des enquêtes menées par des autorités et des administrations.

Il s'agit plutôt de faire des choix sur les futures procédures judiciaires qui seront engagées.

1 - La réquisition judiciaire en droit français est un mécanisme prévu par le code de procédure pénale (articles 60-1 et 60-2, 77-1-1, 77-1-2, 99-3, 99-4, etc.) permettant aux officiers de police judiciaire, procureurs et juges d'instruction d'obtenir communication de documents ou d'informations spécifiques, de la part d'une personne, d'un organisme, d'un établissement ou d'une administration. Le fait de ne pas répondre dans les plus brefs délais à une réquisition judiciaire est passible d'une amende.

2 - Le site de l'AMF https://www.amf-france.org/