



Entreprises victimes de cyberattaques : la stratégie du dépôt de plainte

Myriam Quémener, magistrat au parquet général de la Cour d'appel de Versailles, Expert pour le conseil de l'Europe et l'ONUDC en matière de cybercriminalité (*)

Pouvez-vous nous présenter brièvement vos fonctions de magistrat au parquet général de la Cour d'appel de Versailles ?

Cela consiste à préparer des dossiers d'Assises et à défendre les intérêts de la société dans le cadre d'affaires criminelles concernant les mœurs, les crimes et, de plus en plus, les affaires de criminalité commises en bande organisée ou par l'usage d'Internet (escroquerie, phishing, vols de numéros de carte bancaire, piratage informatique, contrefaçon, pédopornographie, trafic de stupéfiants, sans oublier le terrorisme). A ce sujet, avec ma collègue, procureur adjoint de la cour d'appel de Versailles, nous développons actuellement de nouvelles stratégies procédurales pour ce type de contentieux.

Par ailleurs, en 2009-2010, j'ai piloté un groupe de travail de politique pénale pour améliorer le traitement judiciaire des procédures cybercriminelles dont j'ai dressé le bilan fin 2010. Le constat montre qu'il y a de plus en plus de procédures initiées par les entreprises, en particulier en matière de phishing et d'attaques informatiques.

En quoi consiste les stratégies procédurales que vous avez initiées en matière de cybercriminalité ?

En ce qui concerne la cour d'appel de Versailles, nous essayons de définir avec de grands groupes victimes de cyberattaques, une stratégie de procédure dans des affaires dont le préjudice est extrêmement élevé et les conséquences en termes d'image de marque, non moins importantes. Par exemple, nous avons actuellement plusieurs procédures au bureau des enquêtes concernant la société Microsoft. Avant d'ouvrir une information judiciaire, nous évaluons avec la direction juridique du groupe, la pertinence de regrouper des plaintes au niveau national pour donner de la consistance à la procédure. C'est beaucoup plus efficace que d'avoir une convocation par officier de police judiciaire (COPJ).

Dans le ressort de Versailles nous avons la chance d'avoir les offices qui sont sur Nanterre (CTIC). Les offices centraux, sont des structures de coordination et d'enquête, à compétence nationale qui relèvent de la direction centrale de la police judiciaire (DCPJ). Il en existe une dizaine en France. Ils sont chargés d'enquêtes demandant une technicité policière et juridique. Ils ont développé une politique de contact avec les entreprises en amont, et sont à même d'apprécier le meilleur moment du dépôt d'une plainte. C'est un peu la particularité de ce type de contentieux. Il faut une stratégie !

Qu'avez-vous à dire aux entreprises qui ont encore des réticences à porter plainte ?

Les entreprises sont de plus en plus visées. Les menaces en ligne vont du simple blocage d'accès à des ressources jusqu'au vol d'information et d'identité en passant par l'espionnage, voire l'extorsion d'argent (rançons). Même si le dépôt de plainte n'est pas un acte anodin pour une entreprise, il convient de traiter ces attaques sérieusement, en l'occurrence par un dépôt de plainte auprès des services spécialisés comme la Brigade d'Enquêtes sur les Fraudes aux Technologies de l'Information (BEFTI) ou l'Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication (OCLCTIC). Pour cela il faut rassembler un maximum d'éléments de preuve.

(*) Coauteur, avec Yves Charpenel, avocat général à la Cour de cassation de « [Cybercriminalité, droit pénal appliqué](#) » Economica, Sept. 2010 ; et sous la direction de Chantal Cutajar, « [Garantir que le crime ne paie pas](#) », PUS, Janv. 2011.