Les conditions et sanctions du chantage selon le code pénal et sa preuve par SMS ou sur internet

publié le **11/11/2011**, vu **178627 fois**, Auteur : Anthony BEM

Le code pénal fixe à la fois les conditions du délit de chantage (1) et ses sanctions (2). La jurisprudence récente pose les principes relatifs à la validité de la preuve d'une infraction pénale par SMS ou sur internet (3).

1) Les conditions du délit de chantage selon le code pénal

L'article 312-10 du Code pénal dispose que :

> *« Le chantage est le fait d'obtenir, en menaçant de révéler ou d'imputer des faits de nature à porter atteinte à l'honneur ou à la considération, soit une signature, un engagement ou une renonciation, soit la révélation d'un secret, soit la remise de fonds, de valeurs ou d'un bien quelconque ».*

Ainsi, selon le code pénal, pour que le délit de chantage soit constitué il nécessite :

- l'emploi d'un moyen tel que la menace de révéler ou d'imputer des faits portant atteinte à l'honneur ou à la considération.

- une menace écrite ou verbale, adressée à la victime ou bien à un tiers.

- une menace antérieure à la révélation. Mais le délit peut être aussi constitué lorsque les faits ont déjà été révélés à faible échelle, sont tombés dans l'oubli, ou enfin si s'ils ne leur a été initialement portés aucun crédit.

- une révélation qui doit porter sur des faits précis et qui ne permettent pas d'avoir de doute sur la réalité des faits que le "maître chanteur" menace de révéler. Peu importe que le fait soit exact ou faux.

- cette révélation doit porter sur des faits de nature à porter atteinte à l'honneur ou à la considération. Il importe peu que le fait soit exact ou non du moment qu'il est de nature à porter atteinte à réputation, la probité, à la position sociale ou l'e-réputation de la victime. S'agissant des menaces de violence en cas de non paiement de somme d'argent, elles ne sont pas constitutives de chantage au sens du code pénal mais de tentatives d'extorsion de fonds ou de menaces de violences contre une personne ou ses biens en fonction des situations.

- La poursuite d'un but tendant en l’obtention d’une signature, d’un engagement, d’une renonciation, la révélation d’un secret, la remise de fonds, de valeurs ou d’un bien quelconque. S'agissant de la remise de fonds, il peu importe que le montant soit déterminé ou non.

- enfin une intention coupable, c'est à dire la volonté ou la conscience d’utiliser des menaces illégitimes pour obtenir la remise indue d’une chose. Ainsi, il n'y aura pas d'intention coupable et donc de chantage lorsque qu'une victime demande le versement d’une somme d’argent contre renonciation à sa plainte en guise de transaction ou lorsque la menace est de recourir aux voies légales pour obtenir le paiement de sa dette.

2) Les sanctions du délit de chantage selon le code pénal

L’article 312-10 du Code pénal prévoit que la peine encourue pour le délit de chantage ou sa tentative est de cinq ans d’emprisonnement et de 75.000 € d’amende maximum.

Par ailleurs, lorsque l’auteur de l’infraction aura mis sa menace à exécution l’article 312-11 du même code prévoit qu'il s'agit d'une circonstance aggravante dont les peines encourues sont de sept ans d’emprisonnement et de 100.000 € d’amende maximum.

Enfin, le législateur a prévu d'éventuelles peines complémentaires à l'encontre de l'auteur telles que l’interdiction d’exercer une fonction publique, l’interdiction d’exercer les droits civiques ainsi que toutes celles prévues aux dispositions de l'article 311-12 du code pénal.

3) La preuve d’une infraction pénale par SMS ou sur internet

Internet et les courriers électroniques vulgairement appelés « emails » sont devenus le moyen de communication le plus utilisé et respectivement le lieu de commission et le moyen de commission de nombreuses infractions pénales telles que les propos racistes, diffamatoires ou injurieux, la diffusion de photographies ou vidéos à caractère pédophile ou personnelles mais aussi les menaces ou le chantage toutes les fois où le maitre chanteur n’aura pas été assez *maître dans son art* .

A cet égard, l'article 1316-1 du Code civil dispose que :

> *« L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité ».*

Le fait qu'un courrier électronique puisse être utilisé comme mode de preuve ne fait dès lors pas de doute, à condition qu'il soit signé pour garantir l'intégrité de son contenu et l'identification de son auteur.

Dans le cadre des procédures pénales, la chambre criminelle de la cour de cassation a jugé à plusieurs reprises que *« aucune disposition légale ne permet aux juges répressifs d'écarter les moyens de preuve produits par les parties au seul motif qu'ils auraient été obtenus de façon illicite ou déloyale, il leur appartient seulement d'en apprécier la valeur probante après les avoir soumis à la discussion contradictoire »* (Cass. crim., 13 oct. 2004).

Lorsque l'e-mail produit à titre de preuve n'est pas signé, ce qui est souvent le cas dans les litiges, la question de la fiabilité technique se pose avec le plus d'acuité. Il en est ainsi dans les affaires en droit de la famille, en droit du travail et en droit pénal.

La personne soupçonnée d'avoir envoyé le mail litigieux pourra invoquer plusieurs types de défense pour mettre en doute la fiabilité d'un courriel.

Elle pourra tout d'abord prouver qu'elle n'était pas présente à son poste informatique à l'heure d'envoi du mail, ce qui n'est pas tâche facile.

En cas d'impossibilité d'apporter cette preuve, la personne pourra démontrer que d'autres personnes (époux, secrétaire, administrateur de réseau, tiers) ayant accès à son mot de passe auraient pu se connecter à son poste informatique et envoyer l'e-mail litigieux à partir de ce poste.

Si un mot de passe avait été mis en place, la personne soupçonnée pourra invoquer le fait que l'usurpateur a forcé son mot de passe et s'est introduit dans son poste informatique.

En effet, Eric Charton, dans un ouvrage intitulé Hacker's guide indique qu'*« absolument tous les mots de passe créés par des logiciels fonctionnant sous Windows mais aussi sur Mac et sur des ordinateurs sous Linux peuvent être décodés par un contre-logiciel de décryptage spécialisé : il suffit de le trouver sur Internet, et il est souvent gratuit »* (éd. Campus Press, 2003, p. 175*).*

Ainsi, il existe divers moyens afin de faire tomber la preuve par email ou par SMS, de sorte qu'il convient de s'armer d'un avocat spécialisé en la matière pour ne pas courir de risque dans le cadre de la procédure judiciaire en produisant une preuve viciée.

A titre d'exemple, le 27 mai 2011, le Tribunal de grande instance de Paris a écarté des débats, en tant que preuve, les constats d'huissier réalisés à partir d'un site d'archivage car, d'une part, il s'agissait d'un site « exploité par un tiers à la procédure, qui est une personne privée sans autorité légale, et dont les conditions de fonctionnement sont ignorées » et, d'autre part, non respect des « diligences techniques permettant de s'assurer que les pages visitées n'ont pas été conservées dans la mémoire cache de l'ordinateur et du serveur proxy ». (Tribunal de grande instance de Paris 3ème chambre, 2ème section, 27 mai 2011, Legende Llc et autres / MG Demand Holding et autres)

Les juges ont ainsi considéré que :

> « *il résulte de la lecture du constat d'huissier que* ***si l'huissier instrumentaire a bien procédé aux démarches de suppression des fichiers historiques et des caches, sans toutefois procéder aux impressions d'écran correspondantes ni supprimer les cookies, il n'a accompli cette démarche qu'une seule fois avant son intervention alors que les opérations se sont déroulées en trois étapes et que les constats réalisés, notamment sur le site internet eBay n'ont pas été précédés des mêmes diligences techniques permettant pas de s'assurer que les pages visitées n'ont pas été conservées dans la mémoire cache de l'ordinateur et du serveur proxy et que l'affichage porté à l'écran était bien d'actualité .***

> *… l'huissier indique en page 6 du même constat avoir "stoppé cette nouvelle commande, mais en avoir imprimé le cheminement" puis avoir "imprimé les pages s'affichant au cours de mes constatations" alors que* ***les 29 pages qui suivent ces mentions ne permettent aucunement de tracer ce cheminement employé pour arriver aux pages imprimées et de faire le lien entre les différentes pages visitées et l'achat du parfum litigieux*** *;*
>
> *Attendu que ces éléments suffisent, sans qu'il soit besoin d'examiner les moyens supplémentaires des parties, à* ***retirer toute force probante au constat d'huissier*** *sur lequel est fondée l'action … ».*

L'évolution des contentieux liés à l'Internet a conduit les juges à établir un véritable droit jurisprudentiel relatif aux conditions de validité des constats établis pour rapporter la preuve d'un contenu litigieux sur Internet.

Progressivement, les juges ont forgé les règles de validité applicables aux preuves des contenus présents sur Internet.

En effet, la preuve internet doit respecter en certain nombre de pré-requis techniques qui permettent de s'assurer de sa fiabilité.

A défaut de respecter ces mesures techniques, c'est non seulement la preuve Internet qui est nulle mais surtout c'est l'action judiciaire engagée qui est vouée à l'échec.

La liste des formalités techniques à réaliser avant de constater des faits ou du contenu litigieux sur internet nécessite de véritables connaissances en informatique.

Les pré-requis techniques à respecter avant de procéder à des constatations en ligne sont notamment de :

Mentionner l'adresse IP de l'ordinateur ayant servi aux constatations.

En effet, l'adresse IP *« permet en cas de litige de vérifier au moyen du journal de connexion du serveur interrogé les pages réellement consultées pendant les opérations de constat ».*

Vider le système de cache du logiciel de navigation utilisé entre chaque connexion à un nouveau site internet.

En effet, le non-respect de cette procédure ne permet pas d'écarter *« l'hypothèse selon laquelle ce sont des pages web situées dans les caches de l'ordinateur qui ont, en fait, été consultées ».*

Vider les autres systèmes de *« cache »* de l'ordinateur tels que l'historique des saisies ou le fichier des cookies.

Déconnecter l'ordinateur de tout serveur proxy utilisé pour les constatations.

En effet, le serveur proxy *« peut permettre l'accès à des pages web qui n'existent pas ou qui n'existent plus sur le site cible à la date des constatations ».*

Imprimer les copies d'écran au fur et à mesure des constatations.

Décrire le type d'ordinateur sur lequel l'huissier de justice ou l'expert a opéré ses constatations, son système d'exploitation et son navigateur.

Vérifier la synchronisation de l’horloge interne.

Ces règles s’imposent à toute personne procédant à des constatations en ligne, quelle que soit sa qualité huissier de justice, agents assermentés de l’Agence de protection des programmes ou du Celog.

Or, je me permets d'attirer l'attention de chacun sur le fait que nombre d'huissier de justice s'improvisent expert informatique afin de faire face aux demandes de plus en plus nombreuses de constats Internet mais sans avoir les compétences techniques requises à cet effet.

Enfin, si ces règles strictes conditionnent la finalité du procès elles supposent aussi de faire appel à un avocat spécialisé qui s’assurera de leur respect et qui en contrôlera celui de la partie adverse soumise aux mêmes règles de preuve en vertu du principe du parallélisme des formes.

Je suis à votre disposition pour toute information ou action.

PS : Pour une recherche facile et rapide des articles rédigés sur ces thèmes, vous pouvez taper vos "mots clés" dans la barre de recherche du blog en haut à droite, au dessus de la photographie.

Anthony Bem
Avocat à la Cour
27 bd Malesherbes - 75008 Paris
Tel : 01 40 26 25 01

Email : abem@cabinetbem.com

www.cabinetbem.com