LesEchos.fr

Internet : gare au vol d'identité

Par ***Laurence Neuer*** | 28/06 | 07:00

jérome meyer-bisch pour « les echos »

Ce cadre dirigeant pensait être assez méfiant vis-à-vis des réseaux sociaux. Il s'est pourtant fait piéger. Plusieurs cadres d'une entreprise bien connue l'avaient sollicité sur un réseau professionnel très sérieux. Ils voulaient obtenir des informations sur les tarifs pratiqués par son employeur en matière de certains services personnalisés. Il a été coopératif, mais il s'est bien gardé d'être trop prolixe. Du coup, les réponses ont déplu aux internautes. Ils se sont vengés en dénigrant leur correspondant et en jetant le discrédit sur son entreprise.

En réalité, les goujats ne travaillaient absolument pas pour la société dont ils se réclamaient. Ils n'avaient qu'une idée en tête : abîmer l'image de concurrents potentiels. En l'espèce, ils ont fait deux victimes : l'entreprise qui leur a servi de prête-nom et celle qui a été dénigrée pour avoir refusé

de donner les clefs du coffre. Face à cette calamité qui prolifère, juristes et experts déchiffrent les façons de se défendre.

1 Figer la preuve

C'est que le Web est devenu un vivier de données sur les entreprises et leurs collaborateurs. D'autant que *« certaines personnes, pour se faire mousser, n'hésitent pas à donner beaucoup de détails sur leurs fonctions et responsabilités »,* observe Hubert Moineau, conseil en gestion de risque, dirigeant de +Mitigate. Le réseau est donc un vecteur potentiel d'usurpations d'identités. Hormis les cas de « hacking » (consistant par exemple à forcer les verrous de sécurité d'un site pour voler des mots de passe), *« c'est le plus souvent l'internaute qui fait rentrer le loup dans la bergerie »*, souligne Anne Souvira, chef de la brigade d'enquête sur les fraudes aux technologies de l'information (Befti).

Mais une fois piégée, que doit faire la victime ? Le constat d'huissier est un bon réflexe car il permet de figer la mémoire - par nature volatile -de l'Internet. Mais cette preuve est sujette à caution en raison de l'orthodoxie requise en la matière. Mieux vaut solliciter la nomination d'un expert par voie de requête (article 145 du Code de procédure civile), ce qui suppose d'obtenir du juge qu'il ordonne au réseau social de communiquer les données d'identification du faussaire. C'est la voie qu'avait suivie l'humoriste Omar Sy avant de poursuivre celui qui s'était fait passer pour lui sur Facebook.

2 Porter plainte

« Le risque d'une telle démarche est que le juge rejette la demande car il ne la considère pas suffisamment fondée, prévient Claire Le Touzé, avocate au cabinet Simmons & Simmons. *En outre, au civil, c'est le demandeur qui conduit l'enquête et réunit les preuves qui seront nécessaires à l'obtention de dommages et intérêts. »* Plus efficace, moins coûteuse, et plus sûre du point de vue de la preuve, la voie pénale doit être privilégiée dans ce cas de figure. D'autant que *« la Befti dispose de moyens d'investigation qui n'existent pas au plan civil »*, précise M ^{e} Le Touzé. Une simple déposition auprès des services de police suffit à déclencher l'enquête. Mais la victime peut aussi écrire au procureur ou, si sa plainte n'est pas suivie d'effet, peut déposer plainte contre X en se constituant partie civile entre les mains du juge d'instruction. Seul inconvénient du pénal, *« on ne tient pas les rênes de l'enquête »*, indique M ^{e} Le Touzé. La victime contribue néanmoins à orienter les investigations grâce aux indices livrés aux enquêteurs. Ainsi, un plan social récent ou un prestataire de services éconduit peuvent fournir des pistes précieuses aux enquêteurs. Reste qu'un mirage de dernière minute n'est pas exclu. *« Il arrive que le véritable auteur ne soit pas celui dont on a identifié l'adresse IP mais quelqu'un qui se sera introduit frauduleusement dans son réseau informatique »*, explique Anne Souvira.

3 Classifier l'infraction

En l'espèce, les conclusions de l'enquête de police permettront au procureur de peser l'opportunité de poursuivre le ou les auteur(s). Les faits pourraient relever de la tentative d'escroquerie (article 313-1 du Code pénal). Encore faut-il démontrer l'existence de *« manoeuvres frauduleuses »* procédant de *« l'usage d'un faux nom ou d'une fausse qualité »* et destinées à se faire remettre des « fonds », des « valeurs » ou un « bien quelconque ». *« L'information est susceptible de faire partie de la "valeur" patrimoniale de l'entreprise »*, précise Anne Souvira. Est-elle pour autant un « bien » au sens juridique du terme ? *« La question du vol de données immatérielles fait l'objet d'un débat jurisprudentiel,* précise Myriam Quemener, magistrat et spécialiste de la cybercriminalité. *Prévoir une infraction de vol de bien immatériel comme c'est déjà le cas pour le vol d'électricité serait une adaptation pertinente du Code pénal. »* Les faux profils dont se réclament les auteurs peuvent aussi être épinglés au titre de l'usurpation d'identité en ligne, délit passible d'un an d'emprisonnement et de 15.000 euros d'amende (article 226-4-1 du Code pénal). La victime pourra, par ailleurs, solliciter des dommages et intérêts, mais *« ce qui importe avant tout pour elle, c'est la condamnation de l'auteur »*, souligne M e Le Touzé.

LAURENCE NEUER

À retenir
L'internaute est l'**acteur de sa propre sécurité** : « Il doit donc limiter la divulgation d'informations personnelles ou sur la société.
Contacté sur un réseau, l'internaute doit prendre le temps de **comprendre les demandes** qui lui sont adressées et de recouper l'information en utilisant un autre vecteur que l'Internet tel que le téléphone. »