L'utilisation de logiciels espions par la police est controversée

Pour l'avocat Sébastien Fanti, les polices fédérales et cantonales ne devraient pas pouvoir mettre en œuvre des «chevaux de Troie» sans base légale expresse. Le procureur Jean Treccani et Sylvain Métille, docteur en droit, estiment, au contraire, que ces investigations, strictement encadrées, sont possibles.

On les appelle des «chevaux de Troie», car ces logiciels espions, d'apparence légitime, permettent de prendre le contrôle à distance d'un ordinateur cible, afin d'en surveiller, en temps réel, tout ce qui s'y passe. A la manière des Grecs, qui s'étaient cachés dans un gigantesque cheval de bois pour entrer par ruse dans la ville de Troie, les chevaux de Troie informatiques sont utilisés pour suivre en direct les discussions par messagerie instantanée ou via la téléphonie par internet (type Skype). Ils peuvent transmettre des captures de ce qui se passe sur l'écran de l'ordinateur infecté, activer sa webcam ou son micro et même indiquer les touches frappées (ce qui permet de connaître les mots de passe de l'utilisateur visé).

La police judiciaire fédérale a eu recours dans trois cas de lutte antiterroriste et dans un cas de criminalité organisée à un logiciel destiné à décrypter des contenus codés, oraux ou écrits, a indiqué le Département fédéral de justice et police. De son côté, le canton de Vaud a arrêté un pédophile grâce à ces programmes, et le canton de Zurich a utilisé ce moyen pour lutter contre un important trafic de drogue.

DR

Sylvain Métille

Les quatre cas d'utilisation par la police fédérale sont intervenus avant l'entrée en vigueur du nouveau Code de procédure pénale suisse (CPP), sur la base de l'art. 66 II de la loi fédérale de 1934 sur la procédure pénale, aux termes duquel le juge d'instruction ou le procureur général peut ordonner l'utilisation d'«appareils techniques de surveillance». Le nouveau CPP a repris cette formule à l'art. 280 CPP, qui dispose que le Ministère public peut utiliser des dispositifs techniques de surveillance aux fins, notamment, d'écouter ou d'enregistrer des conversations non publiques. «Cette disposition vise apparemment les écoutes, observations et enregistrements au moyen d'appareils acoustiques et/ou optiques», signale Jérôme Bénédict, avocat à Lausanne et rédacteur du chapitre consacré aux preuves illégales dans le Commentaire romand du CPP. «Or pénétrer dans un système informatique va plus loin. Un logiciel n'est pas un appareil. Pour moi, l'utilisation de chevaux de Troie n'a, pour l'heure, pas de base légale, car le législateur n'y a pas pensé. Le fait que l'avant-projet de loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT) prévoie une base légale expresse pour l'interception et le décryptage de données à son art. 270bis est un in-

Une preuve illégale?

Si un tribunal venait à admettre que les preuves obtenues en utilisant un cheval de Troie l'ont été en violation du droit de procédure pénale, car la base légale actuellement existante est insuffisante à cet effet, l'intéressé pourrait se plaindre d'une violation de son droit constitutionnel à la liberté personnelle. «Nous serions dans une situation que le législateur n'a pas réglée et, dans un tel cas, le juge procéderait sans doute à une pesée des intérêts, précise Me Jérôme Bénédict, spécialiste de cette question: Il est vraisemblable qu'il estime l'atteinte justifiée si l'on est en présence d'une infraction grave, qui ne pouvait être décelée d'une autre manière.» Reste le problème de la provenance de ces chevaux de Troie, qui peuvent constituer des produits illicites s'ils sont développés par des pirates informatiques: un danger dont la police doit évidemment se garder.

DR

Les chevaux de Troie informatiques sont utilisés pour suivre en direct les discussions par messagerie instantanée ou via la téléphonie par internet (type Skype).

dice qu'une telle utilisation pose problème du point de vue de sa licéité.»

«Pas d'interprétation extensive»

«Je ne veux pas d'une interprétation extensive de la loi», déclare de son côté l'avocat valaisan Sébastien Fanti, spécialiste des nouvelles technologies. «Aux Etats-Unis, ces pratiques policières sont répandues, mais les agents disposent du Patriot Act, une base légale spécifique permettant d'accéder à ces informations. Pour moi, en Suisse, la police ne devrait rien pouvoir faire avant l'entrée en vigueur de l'art. 270bis nouveau CPP pour ne pas s'exposer au risque d'abus d'autorité. S'agissant de la surveillance de particuliers, une interprétation plus large de la loi n'est pas possible. En outre, des problèmes concrets se posent: le porte-parole de la police cantonale vaudoise a confirmé avoir développé des partenariats avec plusieurs hautes écoles du canton, afin d'élaborer des logiciels espions pour effectuer des écoutes téléphoniques, intercepter des SMS et des données de géolocalisation», rapporte encore Sébastien Fanti. Il estime que, «du point de vue du droit d'auteur, ces systèmes ne devraient être développés qu'avec l'aval des fabricants du programme d'ordinateur affecté par les chevaux de Troie. Le risque d'abus est important, car qui nous dit que ces étudiants ne copieront pas le logiciel développé?» L'avocat valaisan évoque encore la crainte que «les pigeons soient pris par ce système, mais non les spécialistes du cryptage de données, qui renforceront leurs barrières».

Genève, Fribourg et le Valais l'utilisent déjà

Le procureur général adjoint vaudois Jean Treccani est l'auteur d'un article consacré à cette question, qu'il a cosigné avec le spécialiste Jérémie Müller et le procureur Olivier Jotterand, qui pourrait paraître dans la revue en ligne Weblaw. «J'ai toujours estimé que la base légale était suffisante dans la LSCPT, puis dans le CPP unifié pour fonder certaines opérations, tels l'interception de flux Internet ou l'enregistrement d'actions privées par la webcam ou le micro de l'ordinateur, explique Jean Treccani. La question est de savoir si cette base légale me permet l'accès à l'ordinateur du prévenu pour y déposer le logiciel espion. Je pense que cela est acceptable, au même titre qu'on trouve acceptable d'endommager la porte d'une habitation pour y accomplir une perquisition. Ne pas admettre l'utilisation du cheval de Troie, c'est réduire gravement les moyens d'investigation, puisque c'est le seul moyen d'intercepter des communications cryptées.» La position de Jean Treccani s'oppose à celle d'un autre procureur, le Saint-Gallois Thomas Hansjakob, qui estime que l'art. 280 CPP n'est pas une base légale suffisante pour introduire des programmes informatiques dans une base de données.

Pour Jean Treccani, des limites sont certes nécessaires: «Il faut que le Tribunal des mesures de contraintes définisse exactement le processus qui va être mis en œuvre et il convient de s'interdire toute perquisition clandestine par ce biais.» Il reconnaît que «le sujet est très sensible politiquement, il fait peur au public et nécessite une base légale plus claire pour décourager toute tentative de perquisition sauvage. Il n'en reste pas moins que la base légale actuelle est, à mes yeux, suffisante pour une interception classique de télécommunications ou pour l'enregistrement par webcam.» Il signale que les cantons de Genève, de Fribourg et du Valais ont déjà utilisé ponctuellement un tel moyen, «qui n'est pas facile à installer et très coûteux (entre 10 000 et 20 000 fr.), ce qui constitue déjà un frein à son utilisation. On ne va pas mettre en œuvre un tel moyen sur une petite affaire, mais, si on veut démanteler un important trafic de stupéfiants dans le cadre duquel le logiciel de télécommunication skype est utilisé, cela apparaît comme une nécessité.»

Viser la cible plutôt que le moyen

«Le Code de procédure pénale précise moins les moyens de la surveillance que ce qui en est l'objet, considère Sylvain Métille, docteur en droit et auteur d'un article consacré à la question sur le site weblaw[1]. C'est pourquoi il faut analyser le cheval de Troie selon ce qu'il permet de faire. S'il peut surveiller la transmission d'informations par un ordinateur relié à un réseau de communication (tel qu'internet), il faut le considérer comme une mesure de surveillance de la correspondance au sens de l'art. 270 CPP. Pour que la surveillance ne soit pas disproportionnée, il convient alors de préciser ce qui sera observé (messagerie internet, logiciel de téléphonie, session internet) dans l'ordre donné par le procureur. Si c'est l'environnement qui est observé en activant une webcam ou un micro, la situation est alors semblable au fait de placer des instruments d'écoute dans une chambre, soit d'user d'autres mesures techniques de surveillance, au sens de l'art. 280 CPP. Enfin, effectuer une perquisition à distance en récupérant tout ce qui se trouve sur le disque dur de l'ordinateur, et à l'insu de l'intéressé, n'est pas légal», indique-t-il.

Pour s'assurer que le policier s'en tienne à ces limites, il faut que l'autorisation du Tribunal des mesures de contraintes soit très précise sur ce qui est recherché et autorisé, «car, par méconnaissance technique, ce tribunal risque de donner une autorisation trop large. Il faut aussi s'assurer de l'authenticité des données qui ont été prélevées», met en garde Sylvain Métille.

Sylvie Fischer

[1]Les mesures de surveillance prévues par le CPP: *Quelle place pour le cheval de Troie, l'IMSI-Catcher ou les puces RFID?*, Sylvain Métille, justeletter du 19 décembre 2011, www.jusletter.ch

Une base légale dans le CPP

Dans le cadre de la révision de la loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT), le Conseil fédéral souhaite introduire une base légale plus précise pour l'utilisation de tels logiciels de surveillance de la correspondance et propose, dans son avant-projet de révision de la LSCPT, d'ajouter l'article suivant au Code de procédure pénale:

Art. 270bis Interception et décryptage de données (nouveau)

1 Lorsque, dans le cadre d'une surveillance de la correspondance par télécommunication, les mesures de surveillance prises jusqu'alors sont restées sans succès ou lorsque les autres mesures de surveillance n'auraient aucune chance d'aboutir ou rendraient la surveillance excessivement difficile, le Ministère public peut ordonner, même à l'insu de la personne surveillée, l'introduction dans un système informatique de programmes informatiques permettant d'intercepter et de lire des données. Dans son ordre de surveillance, le Ministère public indique le type de données qu'il souhaite obtenir.

2 L'ordre de surveillance est soumis à l'autorisation du Tribunal des mesures de contrainte.
Le projet de loi et le message ne devraient être rendus publics que l'an prochain.