

BUSINESS INTELLIGENCE

CONVENTION SUR LA CYBERCRIMINALITÉ* : PEUT-ON COORDONNER L'ACTION DE LA JUSTICE ?

Par Thibault du Manoir de Juaye, Avocat à la Cour

* Le point sur la convention du 23 novembre 2001 ratifiée par la France en 2006
Cet article a été réalisé notamment par emprunt au rapport du conseil de l'Europe

Thibault du Manoir de Juaye ►



Le troisième forum international sur la cybercriminalité vient de se tenir à Lille (24 mars 2009). La ministre de l'Intérieur, Michèle Alliot-Marie, y a annoncé un renforcement des moyens matériels et humains, ainsi qu'une modification de la législation, afin de lutter contre la cybercriminalité. Peu de temps avant, le CLUSIF a rendu son rapport 2008 sur la cybercriminalité. C'est l'occasion de rappeler brièvement quelques règles applicables dans le domaine international pour lutter contre la cybercriminalité.

Qui n'a pas vu ces films policiers américains où un délinquant essaie de passer rapidement dans l'État voisin pour échapper à ses poursuivants et sitôt franchi la frontière se met à narguer narquois les policiers, sûr de son impunité.

Même si elle a été reprise par de multiples téléfilms bas de gamme, vulgarisée, cette histoire pose un problème fondamental pour un juriste, celui des limites de la compétence d'un État que l'on peut résumer en « jusqu'où peut-on poursuivre » ? La question se pose avec une acuité particulière dans le cyberspace où il n'y pas de frontière.

Les tribunaux internationaux restent l'exception

La question est loin d'être uniquement une interrogation de juristes comparable à celles existants sur le sexe des anges ou le nombril d'Adam. Elle présente un aspect également moral : peut-on laisser des crimes odieux impunis, notamment ceux commis contre l'humanité sous prétexte qu'aucun pays n'est territorialement compétent ou parce que le pays du lieu de l'infraction refuse de poursuivre.

C'est la raison pour laquelle a été créée la Cour Pénale Internationale dont le but est de promouvoir le droit international, et son mandat est de juger les individus et non les états (qui est du ressort de la Cour Internationale de Justice). Elle n'est compétente que pour les crimes les plus graves commis par des individus : génocides, crimes de guerre, crimes contre l'humanité.

Ont été créés dans sa mouvance plusieurs tribunaux internationaux, sur l'ex Yougoslavie, le Rwanda ou le Liban.

Le dispositif est habilement complété par le principe de compétence universelle : tout pays serait compétent pour juger les crimes les plus graves, comme ceux contre l'humanité. Certains pays exigent néanmoins un lien, comme par exemple la présence du tortionnaire sur le territoire.

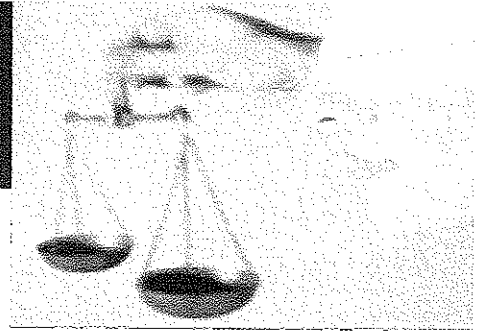
Pour des affaires moins sensibles, chaque pays protège jalousement sa souveraineté

Avant que l'on puisse poursuivre un individu, il faut savoir collecter des preuves pour le confondre et le principe de souveraineté interdit qu'un juge d'un pays enquête dans un autre pays.

C'est la raison pour laquelle il existe un faisceau de conventions pénales internationales prévoyant des systèmes d'entraide de pays à pays.

Toutefois, comment définir dans le monde du cyberspace les pouvoirs d'un juge d'instruction : par exemple, un juge d'instruction français a-t-il le droit de consulter un site Internet basé en Russie sans enfreindre le principe de souveraineté ou doit-on considérer qu'à partir du moment où le juge français a accès à l'information sur l'ordinateur de son bureau, il n'y a pas d'atteinte au principe de souveraineté ?

Il n'y a pas de réponse uniforme à cette question.



Compétence des juridictions d'un pays

Traditionnellement, un pays est compétent en matière pénale, lorsque la victime ou l'auteur de l'infraction est un de ses ressortissants ou lorsque le délit a été commis sur son territoire ou si l'auteur de l'infraction s'y trouve. Mais dans le monde dématérialisé du cyberspace, ces critères peuvent-ils encore être opérants ? A l'évidence non.

Convention sur la cybercriminalité

Pour tenter de résoudre ces différents problèmes, dès le 23 novembre 2001, le Conseil de l'Europe a adopté à Budapest une convention sur la cybercriminalité. Cette convention a été ratifiée par la France en janvier 2006 et est entrée en vigueur en mai de la même année. Il ne faut pas se laisser abuser par l'aspect européen de cette convention puisqu'en réalité de très nombreux pays ont signé ce traité.

La convention va tenter à la fois de régler les problèmes de compétence et d'entraide entre États et obliger à conserver certaines données pour permettre la traçabilité de l'infraction.

Chaque pays signataire est tenu de punir la commission d'infractions établies dans la Convention lorsqu'elles sont commises sur son territoire. Ainsi, par exemple, un pays pourrait revendiquer une compétence territoriale dans le cas où la personne responsable de l'attaque commise contre un système informatique et le système victime de l'attaque se trouvent tous deux sur son territoire, et dans celui où le système informatique attaqué se trouve sur son territoire, même si l'auteur de l'attaque ne s'y trouve pas. Même s'il n'y a pas de définition des cybercrimes ou cyberdélinquances, la convention cite plusieurs infractions pour lesquelles chaque pays signataire doit adopter une législation spécifique. La plupart de ces infractions existaient déjà en droit français de part la loi Godfrain.

■ **Accès illégal** : c'est ce que l'on appelle couramment le hacking. Ces accès illégaux sont souvent le prélude aux activités de vol d'identité ou de phishing. La notion est très proche de celle qui est visée dans l'article 2 de la décision cadre de l'Union Européenne sur les attaques dirigées contre les systèmes d'information. La convention précise que l'acte d'agression doit avoir été commis sans droit et avec intention.

■ **Interception illégale**. Les rédacteurs de la convention ne s'en sont pas cachés, ils ont voulu protéger les interceptions illégales de données informatiques comme il existe une protection pour les correspondances téléphoniques et les enregistrements indus. La convention distingue les communications publiques des communications non publiques. Elle vise même les émissions électromagnétiques provenant d'un système informatique transportant des don-

nées informatiques non publiques !! Le terme 'non publique' qualifie la nature du moyen de transmission (communication), non la nature des données transmises. Il peut arriver que les données transmises soient disponibles pour tout le monde, mais que les participants souhaitent communiquer de façon confidentielle. Les données peuvent aussi être tenues secrètes à des fins commerciales jusqu'à ce que le service ait été rémunéré, comme pour la télévision payante. Il s'ensuit que le terme 'non publique' n'exclut pas en soi les communications par le biais des réseaux publics. Les communications de salariés, à des fins professionnelles ou non, qui constituent des « transmissions non publiques de données informatiques » sont aussi protégées contre l'interception sans droit en vertu de l'article 3 (voir, par exemple, l'arrêt rendu par la CEDH dans l'affaire Halford c. Royaume-Uni, 25 juin 1997, 20605/92) (cf rapport explicatif de l'union européenne).

■ **Atteinte à l'intégrité des données**. Le terme « altération » signifie la modification de données existantes. L'introduction de codes malveillants tels que des virus ou des chevaux de Troie relève donc des dispositions de ce paragraphe, de même que la modification des données qui résulte de cet acte.

■ **Atteinte à l'intégrité des systèmes**. C'est ce que l'on pourrait appeler le sabotage informatique. Ce texte a pour objectif de sanctionner l'entrave intentionnelle à l'usage légitime de systèmes informatiques, y compris de systèmes de télécommunications, en utilisant ou en influençant des données informatiques.

■ **Abus de dispositifs**. Ce texte a pour objectif de sanctionner la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition d'un dispositif d'outils spécifiques utilisés pour commettre les infractions visées dans la convention. De plus, sont visés par ce texte incrimine la production, la vente, l'obtention pour utilisation, l'importation, la diffu-

CONVENTION ON CYBERCRIME* IS LEGAL COORDINATION POSSIBLE?

*CONVENTION ON CYBERCRIME DATED

23 NOVEMBER 2001, RATIFIED BY FRANCE IN 2006

BY THIBAUT DU MANOIR DE JUAYE, ATTORNEY-AT-LAW



The third international forum on cybercrime was held in Lill on 24 March 2009. During the forum, the French Minister for Internal Affairs, Michèle Alliot-Marie, announced an increase in material and human resources, and changes in legislation to help combat cybercrime. Just prior to the forum, CLUSII the French information security circle, published its 2008 report on cybercrime. In view of these events it is worth reviewing some of the international rules that apply in the fight against cybercrime.

BUSINESS INTELLIGENCE

sion ou d'autres formes de mise à disposition d'un mot de passe, d'un code d'accès ou des données informatiques similaires permettant d'accéder à l'ensemble ou à une partie d'un système informatique.

■ **Falsification informatique (article 7).** Cet article a pour objet d'insérer une infraction qui soit le pendant de la falsification des documents sur papier. En conséquence, la falsification informatique consiste à créer ou modifier sans autorisation des données enregistrées de façon qu'elles acquièrent une valeur probante différente de ce qu'elles avaient initialement.

■ **Infractions se rapportant à la pornographie enfantine.**

■ **Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes.**

La France a souhaité étendre la convention aux actes de nature raciste et xénophobe, ce qui fut fait par un avenant.

Le corollaire de l'obligation de stockage des données est la possibilité d'y accéder. La convention prévoit donc que les pays signataires, outre l'obligation de conserver certaines données, doivent organiser une procédure ordonnant par exemple aux hébergeurs) la production des données, la perquisition et saisie de données informatiques stockées et la collecte en temps réel de données informatiques.

Les rédacteurs de la convention ont voulu faire preuve de pragmatisme pour faciliter l'entraide entre les pays, prévoyant même des procédures d'urgence. En complément

des moyens habituels de coopération pénale internationale prévus, par exemple, par les Conventions européennes d'extradition et d'entraide judiciaire, la Convention sur la cybercriminalité définit des formes d'entraide correspondant aux pouvoirs définis préalablement par la Convention. Il est même prévu que chaque signataire de la convention désigne un point de contact joignable vingt-quatre heures sur vingt-quatre, sept jours sur sept, afin d'assurer une assistance immédiate pour des investigations concernant les infractions pénales liées à des systèmes et à des données informatiques, ou pour recueillir les preuves sous forme électronique d'une infraction pénale. Cette assistance englobera la facilitation, ou, si le droit et la pratique internes le permettent, l'application directe des mesures suivantes :

a) Apport de conseils techniques;
b) Conservation des données, conformément aux articles 29 et 30;
c) Recueil de preuves, apport d'informations à caractère juridique, et localisation des suspects.

La Convention sur la Cybercriminalité a prévu des consultations régulières des Parties lors d'au moins une réunion annuelle du Comité de la Convention (T-CY). La dernière réunion de ce comité s'est tenue le 12 et 13 mars 2009 avec un ordre du jour chargé. Il était notamment prévu de faire un bilan d'application de la convention et d'examiner les améliorations à apporter. Parmi les sujets étudiés figure en bonne place celui de la compétence des juridictions pour réprimer les infractions. ■ ■ ■

La Convention sur la Cybercriminalité a prévu des consultations régulières des Parties lors d'au moins une réunion annuelle du Comité de la Convention (T-CY).

La dernière réunion de ce comité s'est tenue le 12 et 13 mars 2009 avec un ordre du jour chargé. Il était notamment prévu de faire un bilan d'application de la convention et d'examiner les améliorations à apporter. Parmi les sujets étudiés figure en bonne place celui de la compétence des juridictions pour réprimer les infractions. ■ ■ ■

La protection rapprochée de votre réseau

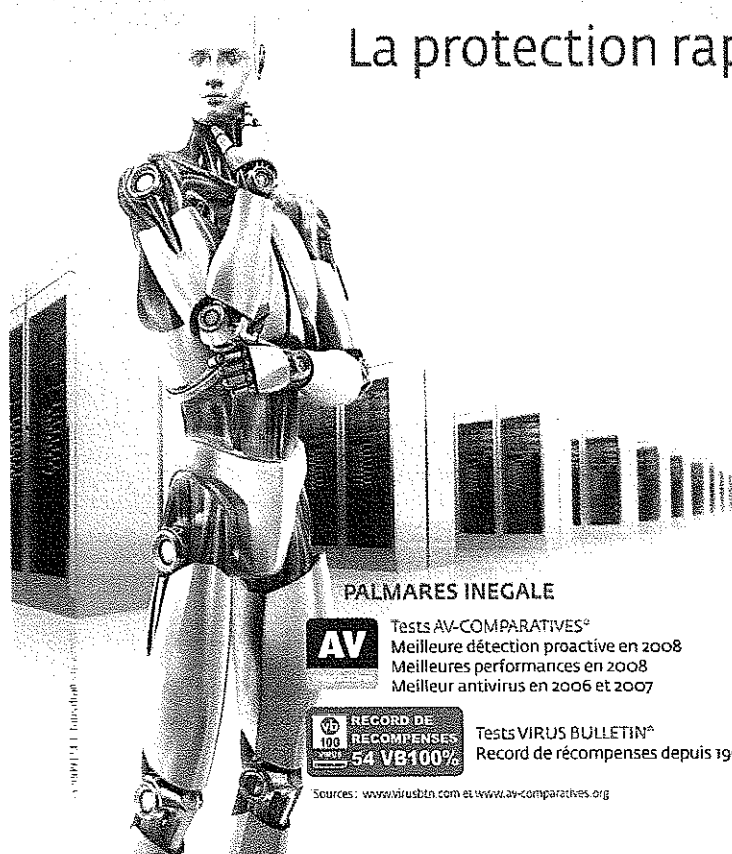
ESET NOD32 Antivirus 4 ESET Smart Security 4

Les plus rapides et légères des protections pour PC

Protégez efficacement votre réseau contre les virus, vers, chevaux de Troie, logiciels espions et publicitaires, rootkits, phishing, et autres menaces évolutives grâce à la nouvelle version 4 des solutions ESET.

Antivirus, Antispyware
Pare-feu
Antispam
Facile à déployer et à administrer

Téléchargez une version d'évaluation sur
www.eset-nod32.fr



PALMARES INEGALE



Tests AV-COMPARATIVES®
Meilleure détection proactive en 2008
Meilleures performances en 2008
Meilleur antivirus en 2006 et 2007



Tests VIRUS BULLETIN®
Record de récompenses depuis 1998

Sources: www.virusbtn.com et www.av-comparatives.org

we protect your digital worlds

