INTERNET

La cybercriminalité sous un verrou

Le premier traité international devrait être signé demain à Budapest.

Une trentaine de pays devrait signer, vendredi, à Budapest, le premier traité international contre la cybercriminalité. Les quinze Etats de l'Union européenne en seront. La signature des Etats-Unis est restée longtemps incertaine. Bien qu'ayant participé à l'élaboration du texte, les Américains considèrent avec beaucoup de circonspection, depuis l'installation de l'administration Bush, toute forme de convention multilatérale. Mais hier, la situation semblait se débloquer et l'accord de 24 pays était déjà assuré.

La Convention de Budapest est le fruit de quatre années de travail, menées dans le cadre du Conseil de l'Europe (43 Etats plus, avec un statut d'observateurs, les Etats-Unis, le Canada, le Japon et l'Afrique du Sud). Elle a trois objectifs. Primo: faire adopter à tous les Etats une définition commune des infractions commises sur et via l'Internet: propagation de virus, intrusion dans des systèmes informatiques, interception illégale, etc. Bref le texte définit un «*noyau dur du cybercrime*», selon l'expression d'un des négociateurs, afin que les droits nationaux parlent la même langue. Deuxio: établir des règles communes pour les enquêtes et les procédures pénales. Elles prévoient notamment la possibilité de mener des «téléperquisitions» (perquisition d'ordinateurs via le réseau), mais celles-ci ne pourront être effectuées qu'à l'intérieur des frontières d'un pays. Ces règles obligent aussi les fournisseurs d'accès à conserver durant au moins trois mois certaines données sur le trafic de leurs clients. Tertio: faciliter la coopération internationale, en créant dans chaque pays un «point de contact» opérationnel 24 heures sur 24, 7 jours sur 7. En France, ce sera l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC).

Racisme. Ce texte touffu (48 articles) a connu 27 moutures successives. Lors du G8 spécial cybercriminalité organisé à Paris en mai 2000, les Etats-Unis ont soutenu l'idée d'une «police transfrontière du Net», qui aurait donné une compétence universelle aux enquêteurs et aux juges. L'Europe s'y est opposée, préférant les procédures d'entraide. Inversement, la France et l'Allemagne ont cherché à inclure dans la convention un article réprimant la propagande raciste en ligne. Les Américains ont freiné des quatre fers, au nom de leur conception de la liberté d'expression. Résultat: un groupe a été mandaté pour écrire, d'ici juin 2002, un «protocole additionnel» sur la répression du racisme en ligne, auquel les pays signataires ne seront pas obligés de souscrire. On peut donc douter de son efficacité. Au bout du compte, les seules incriminations communes en matière de contenus seront la pornographie enfantine et les atteintes à la propriété intellectuelle.

Une version provisoire de la convention, rendue publique au printemps 2000, avait subi un tir de barrage de la part d'associations internationales de protection des libertés. Le texte fut alors complété d'un article rappelant quelques grands principes en matière de droits de l'homme et de libertés fondamentales.

Enquêteur. L'adaptation du droit français à cette convention est un chantier déjà engagé, puisque le projet de loi sur la société de l'information (LSI), dont l'examen par le Parlement est prévu au printemps prochain, intègre la plupart des dispositions du texte de Budapest. Et la loi sur la sécurité quotidienne, récemment adoptée, oblige déjà les fournisseurs d'accès à stocker leurs «données de connexion», susceptibles d'être utilisées par les enquêteurs.

Cette convention rendra-t-elle plus efficace la lutte contre la «délinquance informatique»? Les technologies évoluant sans cesse, le texte du traité devra être régulièrement adapté. Mais sans adhésion massive de la communauté internationale, il sera difficile à mettre en œuvre. Le Canada et le Japon semblent partants. L'Afrique du Sud aurait donné un accord de principe, mais des difficultés techniques pourraient l'empêcher de signer dès vendredi. L'Australie, qui pratique dans le secteur de l'Internet un droit plutôt expérimental, ne s'est pas jointe aux discussions ●

EDOUARD LAUNET

La foire aux mouchards électroniques

Au salon Milipol, l'écoute high-tech veut rester discrète.

Le stand a de la gueule avec son slogan sur panneau bleu: «*In God we trust, the rest we monitor*» (En Dieu nous croyons, le reste, nous l'espionnons). Et l'objet exposé est intriguant: un boîtier à brancher directement sur la ligne téléphonique d'un particulier, capable d'intercepter toutes ses consultations de pages Web et ses e-mails. Mais le responsable de Spectronic Denmark, «*leader mondial de la surveillance électronique*», n'est pas chaud pour détailler les avantages de son mouchard. «*Nous parlons seulement avec les gouvernements*», répète-t-il, usant de son ventre comme d'un bélier pour expulser le curieux de son stand.

Pare-balles. Au Milipol, «*le salon de la sécurité intérieure des Etats*», sorte de Foir'fouille pour flics du monde entier au Bourget (ouverte mardi, elle ferme ses portes vendredi), deux mondes se mêlent. Il y a la partie «salon de l'auto», avec des blondes alanguies sur des capots de véhicules blindés et des mannequins en plastique revêtus de gilets pare-balles dernier cri. Et il y a les officines discrètes de l'écoute high tech. Car la cybercriminalité est à l'honneur avec un nombre croissant de pays qui branchent leurs polices sur le Net, et même un traité international sur le sujet (voir ci-dessus). Du coup, le marché de l'écoute du réseau devient un bon créneau pour toutes les sociétés jusque-là spécialisées dans l'interception téléphonique. La mode est aux clones de Carnivore, le système du FBI capable d'éplucher des milliers d'e-mails pour en extraire les infos utiles aux enquêteurs. Tous présentés avec une discrétion à la mesure de la violente polémique suscitée par Carnivore aux Etats-Unis, entraînant commission d'enquête parlementaire et hurlements d'associations de défense des libertés.

«Marie» est un appareil capable d'intercepter 100 % des messages electroniques, pour peu qu'il soit branché chez un fournisseur d'accès à Internet.

Quelques vitrines de Beretta après les Danois de Spectronic, on trouve une flopée de spécialistes: l'Israélien Comverse Infosys qui détaille ses systèmes d'écoute grâce à de jolis dessins animés, mais dont le responsable du stand ne parlera «*qu'en présence de son vice-président*». Ou Communication et Systèmes, qui, en bon camarade, renvoie vers ses concurrents d'Aqsacom, assurant qu'«*ils installent des systèmes d'interceptions chez les fournisseurs d'accès à l'Internet*». Ceux-ci, bien sûr, ne mouftent pas, «*ce serait une faute professionnelle*».

Intercepter. Chez Arpège Défense, PME du sud de la France spécialisée dans l'écoute en tous genres, téléphones ou satellites, en revanche, on cause un peu. Leurs produits s'appellent «Aurélie» ou «Sissi». Le plus en pointe, c'est «Marie», capable «*d'intercepter 100 % des messages électroniques*», pour peu qu'il soit branché chez un fournisseur d'accès, là où transitent toutes les communications d'un internaute, plastronne Claude Lancial, son responsable commercial. «Marie» est un ordinateur dopé grâce à un logiciel d'analyse du trafic de données. Et réglable selon les besoins du client. «*On peut ainsi capter les communications pour une adresse e-mail donnée, ou par mots-clefs*», explique-t-il. A qui vend-il «Marie»? «*Euh...*» Et combien coûte l'engin? «*Cela dépend, enfin, je ne préfère pas vous le dire.*» En tout cas, il l'assure, virant soudain au rouge pivoine, cela ne sert que pour des «*missions particulières comme le grand banditisme, la drogue ou la recherche de pédophiles*». En France aussi? «*Désolé, j'ai un rendez-vous.*» ●

FLORENT LATRIVE