canton de vaud
LIBERTÉ ET PATRIE

CONSEIL D'ETAT

Château cantonal
1014 Lausanne

Office fédéral de la justice
Unité Droit pénal international
Bundesrain 20
3003 Berne

Réf. : MFP/15004326

Lausanne, le 17 juin 2009

Consultation fédérale relative à l'approbation et mise en œuvre de la Convention du Conseil de l'Europe sur la cybercriminalité

Madame, Monsieur

Par la présente, le Conseil d'Etat du Canton de Vaud répond à la lettre du Département fédéral de justice et police du 16 mars 2009, vous transmettant ses déterminations sur la consultation mentionnée en titre.

D'une manière générale, le Gouvernement vaudois relève que plusieurs aspects importants, dans le projet de législation d'application de la convention, doivent être corrigés, dont notamment les suivants.

- Il importe d'introduire dans le Code pénal une disposition précisant clairement que l'accès indu à un système informatique est également punissable si l'auteur a agi sans dessein d'enrichissement (cf. article 3 de la convention).

- Le délai de conservation des données doit être porté à une année (cf. article 16 de la convention).

- Il convient de prévoir une possibilité de collecter en temps réel les données relatives au contenu du trafic informatique (cf. article 34 de la convention).

Ces appréciations sont développées dans l'annexe jointe au présent courrier (chiffres 2, 4 et 6), de même que d'autres remarques importantes énumérées article par article.

Moyennant ces rectifications à apporter à la législation nationale d'application, le Conseil d'Etat émet un avis favorable à la ratification d'une convention qui tend à l'harmonisation du droit matériel et procédural en matière de cybercriminalité.

Plus particulièrement, le Conseil d'Etat salue la mise en place de procédures simplifiées en matière de transmission de données informatiques, qui permettent d'éviter les longueurs administratives de la commission rogatoire. Il en va ainsi de l'adoption d'une procédure spéciale pour la transmission d'informations tendant à l'identification d'usagers de services de télécommunications, ou encore l'accès transfrontalier à des données stockées, avec consentement de la personne légalement autorisée à les divulguer (cf. art. 32 de la convention). Les nouvelles dispositions devraient donc permettre de réaliser certaines tâches d'instructions dans de meilleures conditions et avec célérité.

En vous remerciant de l'attention portée à la présente, nous vous prions de croire, Madame, Monsieur, à l'assurance de nos sentiments distingués.

AU NOM DU CONSEIL D'ETAT

LE PRESIDENT	LE CHANCELIER
Pascal Broulis	Vincent Grandjean

Annexe mentionnée

Copies

- OAE
- Polcant

ANNEXE A LA REPONSE DU CONSEIL D'ETAT A LA CONSULTATION FEDERALE RELATIVE A L'APPROBATION ET MISE EN ŒUVRE DE LA CONVENTION DU CONSEIL DE L'EUROPE SUR LA CYBERCRIMINALITE

Remarques par articles

1. Article 2 de la convention et modification de l'article 143bis CP

Faisant application de sa réserve à l'art. 2 de la convention (art. 1 al. 3 litt. a de l'arrêté), la Confédération modifie l'art. 143bis CP sur les accès indus à un système informatique, notamment en prévoyant que l'acte ne constitue une infraction punissable que s'il a été commis en violation des mesures de sécurité.

La limitation "… et spécialement protégé contre tout accès de sa part..." prévue à l'alinéa 1 de cette disposition, qui se réfère à l'introduction dans un système informatique appartenant à autrui, étonne. En effet, nombre d'intrusions nocives ou malicieuses dans certains systèmes, surtout chez les particuliers, bénéficient "d'invitations" contenues dans des programmes tout à fait licites ou d'un comportement parfaitement délibéré de l'utilisateur : "vers" informatiques, prise de risque par l'utilisateur qui va consulter des sites dont il sait pertinemment qu'ils sont à risque, etc. ou encore le cas où un utilisateur imprévoyant renonce à se doter ou d'activer des systèmes de sécurité classiques comme les Firewall, les antivirus, les antimalwares ou les antispamms. Un tel système ne serait dès lors aucunement "spécialement protégé contre tout accès" de la part du cybercriminel. L'acte de celui-ci n'en est pas moins dommageable pour autant et l'utilisateur profane mérite d'être aussi bien protégé par la norme pénale qu'un ingénieur en informatique.

2. Article 3 de la convention et modification de l'article 143 CP

Comme déjà mentionné (chiffre 1 ci-dessus), le projet prévoit la modification de l'article 143bis CP. Cette disposition punit actuellement l'accès indu à un système informatique sans dessein d'enrichissement. La modification proposée vise à supprimer cette condition afin de couvrir également les cas dans lesquels l'auteur agit avec un dessein d'enrichissement. Le Conseil d'Etat est favorable à cette proposition.

En revanche, aucune modification de l'article 143 CP n'est prévue. Cette disposition punit la soustraction de données en cas de dessein d'enrichissement uniquement. Il apparaît toutefois peu justifié que le terroriste, toute autre personne malveillante, voire le simple curieux ne soient pas punissables pour de tels actes.

En effet, bien que le "dessein d'enrichissement" soit un moteur important d'actes relevant de la cybercriminalité, l'on observe et constate d'abord dans les faits une volonté délictueuse de nuire ainsi que les impacts de ces attaques.

Les attaques par interceptions de transmissions, en particulier celles perpétrées par "phishing" ("hameçonnage"), conduisent à des dommages parfois graves indépendamment des buts visés par leurs auteurs. L'enrichissement des auteurs de telles attaques n'est pas toujours le préjudice le plus grave pour les victimes. C'est le cas lorsque les attaques produisent des dommages collatéraux ou que l'enrichissement est réparti sur un grand nombre de victimes.

Le Conseil d'Etat considère donc qu'il serait opportun de saisir l'occasion d'une modification législative en cours pour harmoniser les articles 143 et 143bis CP. Il propose dès lors de supprimer l'exigence du dessein d'enrichissement à l'article 143 CP.

3. Articles 6 et 7 de la convention : réserves de l'art. 1 al. 3 litt. c et d de l'arrêté d'approbation

Parmi les réserves projetées par la Confédération, celles de l'art. 1 al. 3 litt. c (relative à l'art. 6 § 3 de la convention) et d (relative à l'art. 7 de la convention) de l'arrêté fédéral laissent perplexes.

En effet, s'agissant du premier cas, il semble que ne pas étendre l'infraction de l'art. 6 § 1 de la convention à la production des dispositifs et mots de passe visés aura pour effet de laisser impunie l'activité même de développement, de recherche et de codage des programmes malveillants, conçus dans le but de commettre les infractions contenues à l'art. 6.

Une seconde interrogation porte sur la condition d'intention frauduleuse, imposée pour la réalisation de l'art. 7 de la convention, qui règle la falsification informatique. La réserve envisagée est encore plus restrictive dès lors qu'elle impose que l'infraction soit commise "dans le dessein de procurer à soi ou à un tiers un avantage ou de causer un dommage".

Si l'on se cantonnait ici à des avantages financiers ou patrimoniaux, cette restriction omettrait la fausse représentation ou la copie de sites ou de programmes authentiques, dans le but d'obtenir des logins, des mots de passe ou autres informations destinées à des usages qui ne procurent pas des avantages strictement patrimoniaux, mais génèrent des usurpations d'identités ou de comptes ("vol" de comptes ou de profil online de jeux vidéo, détournement et diffusion de mots de passe de comptes email, par pure malice ou désir d'encombrer ou de saturer un réseau privé ou public, etc.).

De telles situations n'étant pas admissibles, le Conseil d'Etat propose de supprimer les réserves précitées.

4. Article 16 de la convention : conservation rapide de données stockées

L'obligation de conservation des données permettant d'identifier un utilisateur par les fournisseurs de services est limitée en Suisse à six mois. La pratique a démontré que ce délai était trop court, surtout si des demandes préliminaires doivent être faites à l'étranger (par exemple : obtention d'une adresse IP dans un autre pays dont on doit identifier le détenteur auprès d'un provider suisse).
Il importe que les autorités suisses profitent de l'adaptation de notre légalisation à la convention pour fixer à une année le délai de conservation des données, comme cela est le cas en France, par exemple.

5. Article 19 de la convention : perquisition et saisie de données informatiques

La notion de perquisition dans un deuxième système informatique, en passant par un premier système, telle qu'expliquée dans le rapport explicatif ad art. 19, § 2 de la convention, est assez floue. D'une part, il n'est pas toujours possible à un enquêteur d'identifier le lieu où se trouvent les données du deuxième système informatique. D'autre part, des moyens transparents existent aujourd'hui pour accéder directement, depuis un ordinateur, à des données pouvant se situer n'importe où sur la planète. Quoi qu'il en soit, la possibilité de séquestrer ces données doit être clairement donnée à l'enquêteur qui perquisitionne et une procédure doit être définie pour lui permettre d'obtenir rapidement une extension de l'autorisation en cours de perquisition.

6. Article 34 de la convention et modification de l'article 18b de la Loi fédérale d'entraide en matière pénale (EIMP)

En application des articles 30 et 34 de la convention (divulgation rapide de données conservées / entraide en matière d'interception de données relatives au contenu), le projet prévoit l'ajout d'un article 18b EIMP, aux termes duquel, "l'autorité fédérale ou cantonale chargée de traiter une demande d'entraide peut ordonner la transmission à l'étranger de données relatives au trafic informatique avant la clôture de la procédure d'entraide lorsque les mesures provisoires font apparaître que la source de la communication faisant l'objet de la demande d'entraide se trouve à l'étranger ou que ces données sont recueillies par l'autorité d'exécution en vertu d'un ordre de surveillance en temps réel qui a été autorisé".

Le projet d'article 18b EIMP ne traite que des données relatives au trafic informatique, alors que le message explicatif se réfère également au contenu. Ceci peut prêter à confusion. A lire littéralement le texte du projet d'article 18b EIMP, le Conseil d'Etat comprend que, s'il est expressément fait référence au trafic, le contenu est donc à contrario exclu du champ d'application de la disposition, interprétation confirmée par le rapport explicatif, qui exclut expressément l'extension de la facilité prévue par cette disposition à la transmission des données de contenu, tout en précisant que "les autorités suisses ne pourront pas demander à l'étranger de collecter en temps réel des données relatives au contenu" (cf. ch. 2.3.13 du rapport explicatif, in fine).

L'impossibilité de transmettre aux autorités étrangères de poursuite pénale le résultat d'une interception informatique avant d'en avoir soumis le contenu au justiciable et de lui avoir ouvert les voies de droit – au demeurant souvent utilisées de manière dilatoires en matière d'entraide judiciaire - rendraient souvent de telles mesures vaines d'un point de vue opérationnel. A l'inverse, en vertu du principe de la réciprocité et selon ce que rappelle expressément le rapport explicatif, les autorités suisses devraient s'interdire de requérir des autorités étrangères la transmission en temps réel du contenu des interceptions informatiques requises à l'étranger.
Or, de telles interceptions gagneront en importance à mesure que les criminels, en particulier les trafiquants de stupéfiants et les pédophiles, tireront avantage des moyens de télécommunication modernes, en plein essor avec l'ouverture des téléphones mobiles à Internet.

L'enjeu est plus important qu'il n'y paraît de prime abord puisque, pour autant qu'elle existe a priori, la limite entre la téléphonie et l'informatique s'estompe. Interdire expressément et sans réserve, comme le fait le rapport explicatif, la transmission en temps réel du résultat d'une interception informatique, c'est fermer aussi la porte à la pratique actuelle en matière d'interception téléphonique, où le juge suisse accepte de transmettre en temps réel le contenu des interceptions contre l'engagement formel et préalable de l'autorité étrangère de n'en faire usage comme moyen de preuve qu'après validation dans la procédure suisse, compromis entre les besoins opérationnels et les contraintes juridiques. Cette pratique permet aux autorités suisses, par réciprocité, de solliciter des autorités étrangères qu'elles leur remettent en temps réel les résultats des contrôles téléphoniques recueillis à l'étranger. Elle permet aussi d'atténuer l'incompréhension des autorités judiciaires étrangères.

D'après le Conseil d'Etat, le projet d'article 18b EIMP devrait intégrer la possibilité de transmission en temps réel également du contenu des interceptions, éventuellement avec la réserve d'un engagement formel de la part du pays requérant par lequel celui-ci ne s'en servirait à titre de preuve judiciaire qu'après clôture favorable de la procédure interne d'entraide. Subsidiairement, le rapport explicatif devrait s'abstenir de toutes considérations propres à annihiler la pratique actuelle de l'engagement préalable formel.