

## **LA CONVENTION DU CONSEIL DE L'EUROPE SUR LA CYBERCRIMINALITÉ**

*Alexander Seger*

-----

En matière de cybercriminalité, la première chose à faire pour les Etats est d'élaborer une législation nationale efficace et qui soit en harmonie avec les législations nationales des autres pays afin de permettre une bonne coopération entre les pays. La Convention sur la cybercriminalité du Conseil de l'Europe du 23 Novembre 2001 offre une solution en ce sens. Cette Convention a largement dépassé les frontières de l'Europe puisqu'elle est ouverte à la ratification de tous les pays et, pour cela, nous l'avons notamment fait traduire en langue vietnamienne, laotienne, et bientôt cambodgienne.

La première question qu'il faut se poser est celle de savoir ce qu'est la cybercriminalité. La Convention offre une définition de ce terme à travers deux catégories d'infractions :

- Les infractions matérialisées par les attaques contre le système et les données informatiques. Ce sont les infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques. Cela inclut les virus, spyware et autres programmes malveillants ainsi que les SPAM et les attaques en déni de service.
  
- les infractions commises grâce à l'utilisation du système informatique ou à travers ce dernier. Ces des infractions matérialisées par des actes pornographie infantile, de xénophobie, racisme ou encore les infractions contre la propriété intellectuelle etc.

Cependant cette liste ne peut être exhaustive puisqu'aujourd'hui pratiquement toutes les infractions impliquent l'utilisation d'un système informatique. Ainsi les magistrats ou autres professionnels du droit se doivent d'avoir une connaissance approfondie des systèmes informatiques car les preuves de ces infractions se trouveront

sur un système informatique. Il est nécessaire pour les Etats, à côté de la question de la cybercriminalité elle-même, de traiter la question des preuves électroniques.

La question de la cybercriminalité n'est pas une question nationale mais mondiale. A titre d'exemple, beaucoup de banques du Royaume Uni ont été récemment attaquées par le Vietnam (fishing attack) : ce sont des criminels situés au Vietnam qui, par des moyens informatiques, vont réussir à effectuer des fraudes auprès d'institutions financières anglaises. Ce même type d'attaque c'est également produit du Laos envers l'Europe. Ce sont donc bien des questions transnationales, toutes les sociétés du monde sont concernées.

Pour réagir à ces attaques, du point de vue du droit pénal, il est tout d'abord nécessaire de criminaliser ce type de conduite dans le cadre du droit pénal matériel. En ce qui concerne la procédure, il faut donner aux forces de l'ordre du pays, les moyens d'enquêter, de poursuivre et de juger les cyber-crimes et ce d'une façon efficace. Or le problème avec ce type de criminalité est un problème de temps, il faut pouvoir agir de suite et de manière efficace, ce qui demande des moyens importants et l'intégration de ces dispositions dans les codes de procédure pénale. Enfin, il est nécessaire de permettre une coopération internationale efficace et immédiate ce qui implique d'harmoniser les législations, de faire des provisions et d'établir des institutions pour la coopération policière et juridique.

La Convention sur la cybercriminalité traite de tous ces points et offre, comme il a été déjà mentionné, une solution aux Etats en la matière. C'est une Convention qui a été élaborée par le Conseil de l'Europe, mais elle a été, dès le début, considérée comme instrument international grâce à la participation du Canada, du Japon, de l'Afrique du Sud et des Etats-Unis. Cette Convention a été ouverte à la signature à Budapest en Novembre 2001 et est entrée en vigueur depuis 2004. La Convention a été complétée par un protocole, le protocole sur la xénophobie et le racisme par le biais des systèmes informatiques qui a été ouvert à la signature en Janvier 2003 et est en vigueur depuis mars 2006.

La Convention est structurée de la manière suivante :

Le premier chapitre porte sur les définitions des termes spécifiques en la matière (système informatique, données informatiques, fournisseur de services, données relatives au trafic). Le deuxième chapitre porte sur le droit pénal matériel et le droit procédural. Ici la convention sur la cybercriminalité, contrairement à d'autres traités internationaux, met beaucoup l'accent sur le droit procédural étant donné le caractère spécifique des infractions qu'elle traite. Enfin le dernier chapitre, très important, porte sur la coopération internationale.

## **Chapitre 1 : les mesures à prendre au niveau National**

### *Section 1 : Le droit pénal matériel*

Concernant, tout d'abord, le chapitre sur le droit matériel, il démontre aux pays que ce type de criminalité peut se matérialiser par plusieurs activités :

Les infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques :

- l'accès illégal, ce que l'on appelle également le « hacking »
- l'interception illégale
- l'atteinte à l'intégrité des données
- atteinte à l'intégrité du système
- les abus de dispositifs

On peut donner comme exemple à l'infraction d'atteinte à l'intégrité d'un système, celui de l'Estonie, petit pays en Europe de l'Est. Ce pays dépend beaucoup du système informatique, tellement qu'il s'agit peut être même de la société la plus informatisée du monde. Il y a deux ans, ce pays a dû faire face à une forte atteinte à l'intégrité de tout son système informatique. Toute l'infrastructure s'est retrouvée ainsi entièrement bloquée. Or, à cette époque, la peine pour ce type d'infraction était seulement 6 mois maximum de prison car au moment de la préparation de cette loi, il était impensable pour ce pays que ce genre d'infraction puisse être une infraction importante et causant de sérieuses

conséquences. A la suite de ces événements, l'Etat a modifié sa législation et la peine encourue pour ce type d'attaque, aujourd'hui, est de 5 ans d'emprisonnement.

Les infractions informatiques et celles se rapportant au contenu :

- la falsification
- la fraude,
- les infractions se rapportant à la pornographie infantile

### ***Section 2 : le droit procédural***

Généralement les Etats sont relativement efficaces dans la mise en place du droit matériel, le plus grand problème pour beaucoup d'Etats réside dans la mise en place du droit procédural. Il est important que les forces de l'ordre, et notamment la police, puissent mener des investigations de façon efficace. Pour cela il faut disposer des moyens nécessaires pour préserver les données. Pour cela la Convention offre aux pays signataires en son article 16 des dispositions sur la conservation rapide des données informatiques stockées.

Ex : si la police d'un Etat souhaite enquêter sur une activité suspecte, elle doit pouvoir être dans la capacité de demander à un fournisseur de services de préserver les données immédiatement. Il est nécessaire de préserver tout d'abord les données avant que ces dernières disparaissent, il sera ensuite temps de faire les démarches traditionnelles auprès des juges pour mener plus en profondeur l'enquête. Les articles 16 et 17 de la convention contiennent les dispositions sur ce genre de mesures urgentes.

## **Chapitre 2 : La coopération internationale**

- Il y a tout d'abord des principes généraux comme les principes relatifs à l'extradition (article 24), à l'entraide judiciaire (article 25), à l'information spontanée (article 26) etc.
- Il y a surtout des dispositions spécifiques relatives à la cybercriminalité et à la nature originale des infractions. Il ne suffit pas que les règles de procédures valent au niveau

national, cela doit également être le cas dans un cadre international. C'est par exemple le cas de la conservation rapide des données, la police d'un pays doit pouvoir demander une telle procédure à tous fournisseur d'accès, quel que soit l'Etat dans lequel il se trouve (article 29). Beaucoup d'articles traitent de la coopération internationale efficace afin de la détailler au maximum.

### **Chapitre 3 : les clauses finales**

Généralement les clauses finales sont peu intéressantes dans les conventions, mais ici un article est important : l'article 37. Il permet à tous les pays du monde d'accéder à la Convention. C'est grâce à cet article que la Convention est ouverte à la signature et à la ratification de tous les Etats et non seulement les Etats européens. C'est ainsi que le Laos, la Thaïlande ou encore le Cambodge, peuvent y prétendre. Il est important de souligner que cette convention a été ratifiée par les Etats-Unis. En effet, le plus grand nombre de données proviennent de ce pays donc il est vraiment très important de savoir que ce pays fait partie de la convention contre la cybercriminalité. En utilisant l'article 37 le Chili, la République dominicaine, le Mexique et les Philippines ont été invités à y accéder. Ce qui est important est qu'il y a une centaine de pays (environ 120) qui sont en train d'améliorer leurs législations en utilisant la convention de Budapest comme une ligne directrice ce qui signifie qu'il ne s'agit pas seulement d'une convention de l'Europe mais elle offre un cadre global.

#### *Les avantages de la convention*

Les avantages de cette convention et qu'elle donne une approche nationale cohérente sur les législations en matière de cybercriminalité, elle permet de faciliter le rassemblement des preuves électroniques, les investigations et les enquêtes dans les infractions commises par l'utilisation d'un moyen informatique, non seulement les infractions spécifiques en matière de cybercriminalité mais également toutes les infractions « classiques » commises à l'aide d'un outil informatique (blanchiment d'argent, terrorisme et autres crimes). Elle permet une harmonisation des législations entre les Etats et les pays membre de la Convention sont invités à participer à tous les

travaux du comité consultatif, comité en charge de préparer les éventuels futurs protocoles ou annexes à la convention.

Pour accéder à la Convention, il faut d'abord travailler sur la législation nationale. Au moment de la ratification, la législation conforme à la convention doit déjà être en place, d'où la nécessité de commencer par un travail de modification de la législation. Une fois cette première étape effectuée, le gouvernement de l'Etat candidat doit écrire une demande au secrétariat général du Conseil de l'Europe, à la suite de quoi les Etats parties à la convention vont se consulter. Trois mois après cette consultation, le Conseil de l'Europe invitera l'Etat candidat à accéder et ce dernier sera alors libre de décider les modalités d'accession (la date, etc.).

Même en cas de non ratification de la Convention, cette dernière peut faire l'objet de lignes directrices, loi modèle, pour améliorer la législation nationale. Pour cela, le plus facile est de prendre la convention article par article et de les comparer à la législation nationale. De nombreux pays ont demandé au Conseil de l'Europe d'étudier leur profil et, d'ores et déjà, une quarantaine de profils ont été publiés. Le Conseil de l'Europe a par exemple un profil très détaillé sur le Vietnam, le Cambodge, le Laos et la Thaïlande qui vient d'adopter une loi en la matière. L'exemple de la Roumanie est intéressant car ils ont élaboré une loi spécifique qui est presque la copie conforme de la Convention.

La Thaïlande a adopté une loi assez complète en matière de cybercriminalité en 2007 et le Vietnam a adopté deux articles supplémentaires qui vont entrer en vigueur en janvier 2010 criminalisant l'accès illégal et la fraude du système informatique. Il y aurait encore d'autres articles qu'il faudrait ajouter dans le futur, mais surtout ce qui est nécessaire de faire au Vietnam est, dans le contexte de réforme de la procédure pénale, ajouter des articles similaires à ceux prévus dans la Convention. Le Conseil de l'Europe peut aider les pays dans leurs travaux : si un groupe de travail est formé pour élaborer une nouvelle législation, il est possible de collaborer avec ce groupe de travail et analyser les projets de loi. Des ateliers de formation des personnes membres du groupe de travail sont également envisageables. En Mars 2010, une conférence sur la coopération en matière de cybercriminalité sera organisée à Strasbourg et les pays de la région Asie-Pacifique y sont largement invités.

Il est enfin important de souligner que la lutte contre la cybercriminalité ne peut en aucun cas constituer une excuse pour déroger aux droits fondamentaux. Il faut trouver un juste équilibre entre les questions de sécurité et les droits fondamentaux comme celui à la vie privée. Pour cela, il est nécessaire de traiter la cybercriminalité et la protection des données ensemble et non pas séparément du point de vue des législations.