

L'importance de la collaboration internationale et l'expérience belge dans l'échange d'informations policières et de coopération judiciaire

I. Introduction

1. Comme beaucoup d'inventions humaines, Internet et ses possibilités de transmission massive et ultra rapide de données d'un lieu à un autre ou de diffusion de ces données dans le monde entier peut être utilisé tant à des fins légitimes que criminelles.

Le virus « I love you », par exemple, a fait près de 7 milliards de dollars de dégâts en se propageant dans le monde entier via les courriels.

2. Face à ce phénomène, les forces de police et les autorités judiciaires se retrouvent trop souvent impuissantes à maîtriser cette criminalité d'un genre nouveau, en raison de différents facteurs :

a. Tout d'abord, les frontières physiques des Etats nationaux ne constituent pas un obstacle à ce qu'il est convenu d'appeler les autoroutes de l'information. Cet obstacle existe pourtant pour les services qui sont chargés de lutter contre la criminalité, dont les compétences s'arrêtent aux frontières du pays.

Dans le cas de systèmes informatiques liés entre eux, se présente souvent le cas de figure dans lequel l'enquête doit être étendue à d'autres systèmes, situés dans d'autres pays que ceux où la recherche a physiquement lieu, entravant ainsi les mesures d'enquête qui ont été entreprises.

Parfois même, le caractère international des réseaux engendre des situations dans lesquelles des fichiers sont consultés avant même que les services judiciaires n'aient le temps de réaliser que ces fichiers sont stockés à l'étranger.

Les procédures classiques permettant de poser des actes d'instruction dans le cadre d'une instruction pénale en territoire étranger, telle une commission rogatoire internationale, laissent aux intéressés (ou même automatiquement à leurs systèmes informatiques) suffisamment de temps pour faire disparaître quasi instantanément les données via les canaux de télécommunication.

De ce fait, les procureurs belges ont longtemps renoncé à poursuivre dans le cas d'enquêtes contenant des éléments d'extranéité compte tenu des délais inconciliables avec la célérité requise par la cybercriminalité.

Une première difficulté existe donc au niveau de la compétence territoriale des autorités de police et du pouvoir judiciaire.

b. Il y a plus grave : sur certains points, la procédure pénale existante pourrait ne pas être adaptée aux besoins d'une lutte effective contre la criminalité dans la société d'information.

La caractéristique marquante des éléments de preuve dans les affaires de cybercriminalité est la vitesse à laquelle elles voyagent, ainsi que leur fragilité, qui fait en sorte qu'elles peuvent être détruites, altérées, sauvegardées, copiées, déplacées en un instant.

La technologie est en évolution constante. Le P2P, les botnet et l'avènement de l'IPv6 semblent rendre encore plus difficile de tracer les données illicites. Le concours des

fournisseurs d'accès pour la rétention et donc la communication des données d'accès à peine acquis¹, pourrait déjà ne plus être d'un grand secours ...

Une base juridique adéquate fait parfois défaut lorsque les autorités judiciaires souhaitent procéder à la saisie des données elles-mêmes, indépendamment de leur support.

Une deuxième difficulté est celle de la disponibilité de mesures adaptées à la lutte contre ce type particulier de criminalité qu'est la cybercriminalité.

3. Ces constats font apparaître de manière évidente la nécessité d'intensifier la coopération internationale dans le domaine de la lutte contre la cybercriminalité.

4. La présence des participants à la conférence permettant de penser qu'ils partagent avec leur Etat d'origine, au moins sur le principe, ce point de vue, je ne m'y attarderai pas d'avantage. Je vais plutôt envisager ce qui peut être entrepris pour mettre sur pied, intensifier et optimiser cette coopération.

La première partie de mon exposé évoquera la nécessité d'une harmonisation des dispositions pénales formelles et des techniques. La deuxième partie, les différentes solutions conventionnelles qui sont à la disposition des Etats ou qui peuvent servir de source d'inspiration. Seront ensuite mentionnés quelques exemples réussis de coopération internationale en matière de lutte contre la cybercriminalité. Je terminerai en attirant l'attention sur les dérives possibles d'une coopération internationale intensifiée et sur l'importance du respect des droits fondamentaux des individus.

II. Nécessité d'une harmonisation

2.1. Harmonisation juridique

5. Au niveau international, les questions de procédure pénale liées aux technologies de l'information et de la communication ont seulement été soumises à une réflexion approfondie depuis les années 90. Il n'est dès lors pas étonnant que bon nombre d'Etats ne disposent pas encore d'une réglementation globale dans ce domaine.

6. Une harmonisation des règles matérielles est fondamentale et urgente afin d'éviter que ne se développent des « paradis numériques ».

Onel de Guzman, auteur présumé du virus « I Love You », a été relâché et les poursuites engagées par l'Etat philippin contre ce dernier ont été abandonnées car le droit philippin de l'époque n'incriminait pas ces faits

7. Cette même harmonisation forme également la base indispensable pour fonder une coopération internationale efficace.

En effet, si des lois procédurales et matérielles similaires existent, la coopération se déroule automatiquement plus aisément, même s'il est évidemment souhaitable de prendre d'autres mesures pour faciliter la façon dont cette coopération se réalise.

La condition de la double incrimination sert de fondement juridique à un refus d'entraide, lorsque les

¹ Cf. à cet égard la directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications qui oblige les fournisseurs d'accès à stocker les données de trafic et de localisation pendant une durée supérieure à 6 mois (en Belgique, cette durée est de 12 mois au minimum).

faits à l'origine de la demande de l'Etat requérant ne sont pas réprimés par le droit pénal de l'Etat requis². Il est donc important d'harmoniser les incriminations si l'on veut éviter ceci.

8. D'un point de vue pratique, cette harmonisation pourrait être réalisée par l'adhésion aux conventions existantes :

a. Il s'agit d'abord de la Convention de Budapest contre la cybercriminalité³.

Cette convention du Conseil de l'Europe, premier instrument de droit international conventionnel contraignant spécifiquement élaboré pour lutter contre la criminalité informatique, est ouverte à la signature aux Etats non-membres, ainsi les Etats-Unis ont été parmi les premiers à ratifier cette convention. Une réforme visant à combattre la criminalité informatique, fondées sur les lignes directrices de la Convention, est d'ailleurs en cours en Egypte, l'un des pays pilotes du Programme sur le « Renforcement de l'Etat de droit dans les pays arabes – Projet de modernisation des ministères publics ».

Le but premier de cette convention est d'intensifier la coopération entre les parties à la convention et dans cette optique, elle vise à la fois à :

- harmoniser les éléments des infractions ayant trait au droit pénal matériel national en matière de cybercriminalité, que ce soit les infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques, la falsification et la fraude informatique, les infractions se rapportant à la pornographie infantile ou les infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes.
- fournir au droit pénal procédural national les pouvoirs nécessaires à l'instruction et à la poursuite d'infractions de ce type ainsi que d'autres infractions commises au moyen d'un système informatique ou dans le cadre desquelles des preuves existent sous forme électronique,
- mettre en place un régime rapide et efficace de coopération internationale qui sera envisagé ci-après.

Cette convention est complétée par un protocole additionnel relatif à l'incrimination d'actes de nature raciste et xénophobe, commis par le biais de systèmes informatiques⁴.

A l'issue de la conférence régionale des pays arabes sur la cybercriminalité qui s'est tenue au Caire, les 26 et 27 novembre 2007, une déclaration a été adoptée⁵. Elle recommande, comme la conférence régionale qui s'est tenue à Casablanca les 19 et 20 juin 2007 et durant laquelle la présente contribution a été exposée⁶, aux pays arabes de se servir de la Convention sur la Cybercriminalité comme de modèle pouvant les aider à élaborer la législation nationale dans le domaine de la cybercriminalité.

² Article 2 (b) de la convention du 20 avril 1959 et de la convention du 23 novembre 2001 – cf. infra les réf.

³ Signée le 23 novembre 2001, disponible en arabe sur le site : http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/Convention%20and%20protocol/ETS%20185%20Arab%20_Jan%2008_en.pdf.

⁴ Signé à Strasbourg le 28 janvier 2003, disponible en arabe sur le site : http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/Convention%20and%20protocol/ETS%20189%20Arab%20_Jan%2008_en.pdf

⁵ La recommandation est disponible en arabe sur le site : http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/cy%20activity%20Cairo/CairoDeclarationAgainstCC2007_Arabic.pdf

⁶ La recommandation est disponible en arabe sur le site : <http://www.arabniaba.org/publications/crime/casablanca/recommendations-a.pdf>

- b. L'accord ADPIC⁷ fait obligation aux Etats membres de prévoir des sanctions pénales à l'encontre des actes délibérés de contrefaçon de marques ou de piratage commis à une échelle commerciale. Internet est évidemment un terrain de prédilection de ce type de comportements⁸.
- c. Au niveau de l'Union européenne, la transposition de l'accord a été entamée par la directive du 29 avril 2004, relative aux mesures et procédures visant à assurer le respect des droits de propriété intellectuelle, qui a obligé les États membres à prévoir les procédures nécessaires pour assurer le respect des droits de propriété intellectuelle et appliquer des mesures appropriées contre les auteurs de contrefaçon et de piratage⁹. Ces mesures et procédures doivent être suffisamment dissuasives pour éviter la création d'obstacles au commerce légitime et offrir des sauvegardes contre leur usage abusif.

Pour permettre aux mécanismes de coopération, basés en général sur le principe de double incrimination, de fonctionner de manière satisfaisante, il est indispensable que les différents Etats aient une législation pénale comparable.

L'Union européenne a ainsi estimé que ses Membres doivent avoir une approche commune minimale de la contrefaçon et de la piraterie¹⁰. Il n'existe en effet à ce jour aucune norme pénale commune pouvant servir de base à la lutte contre les atteintes à la propriété intellectuelle au sein de l'Union.

La Commission a donc proposé l'adoption d'une directive du Parlement européen et du Conseil relative aux mesures pénales visant à assurer le respect des droits de propriété intellectuelle¹¹, afin d'y intégrer une harmonisation du niveau minimum des sanctions pénales à l'encontre des atteintes à la propriété intellectuelle¹².

On citera également une décision-cadre du Conseil 2005/222/JAI du 24 février 2005 relative aux attaques contre les systèmes d'information¹³ harmonise les infractions, fixe les pénalités, affirme la responsabilité pénale des personnes morales.

⁷ Article 61, Accord sur les aspects des droits de propriété intellectuelle qui touche au commerce TRIPS/ADPIC, fait à Marrakech le 15 avril 1994.

⁸ Une conférence régionale de POGAR sur la criminalité en matière de propriété intellectuelle se tiendra au royaume du Bahreïn du 13 au 14 avril 2008 sur cette matière, <http://arab-niaba.org>.

⁹ Directive 2004/48/CE du Parlement européen et du Conseil, du 29 avril 2004, relative aux mesures et procédures visant à assurer le respect des droits de propriété intellectuelle, disponible sur le site : http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=fr&type_doc=Directive&an_doc=2004&nu_doc=48.

¹⁰ Document de travail de la Commission - Annexe à la Proposition de décision Cadre du Conseil visant le renforcement du cadre pénal pour la répression des atteintes à la propriété intellectuelle - Évaluation d'impact approfondie {COM(2005) 276 final}, disponible sur le site <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52005SC0848:FR:NOT>.

¹¹ Proposition de directive du Parlement européen et du Conseil du 12 juillet 2005, relative aux mesures pénales visant à assurer le respect des droits de propriété intellectuelle (2005/0127), disponible sur le site : http://europa.eu.int/eur-lex/lex/LexUriServ/site/fr/com/2005/com2005_0276fr01.pdf.

¹² Proposition modifiée de Directive du Parlement européen et du Conseil relative aux mesures pénales visant à assurer le respect des droits de propriété intellectuelle (COM/2006/0168 - COD 2005/0127), disponible sur le site : <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52006PC0168:FR:NOT>.

¹³ Décision-cadre 2005/222/JAI du Conseil, du 24 février 2005, relative aux attaques visant les systèmes d'information, J.O.C.E., 16 mars 2005, L69.

Enfin, la décision-cadre du Conseil du 22 décembre 2003 relative à la lutte contre l'exploitation sexuelle des enfants et la pédopornographie¹⁴ tente d'harmoniser les incriminations en la matière.

2.2. Harmonisation technique

9. L'article 25.3 de la convention de Budapest impose, à raison, que les demandes d'entraide ou les communications s'y rapportant « *passent par des moyens offrant des conditions suffisantes de sécurité et d'authentification (y compris le cryptage si nécessaire)* »¹⁵.

Cela n'est malheureusement pas si simple. Contrairement à la signature électronique, l'expéditeur du message est dépendant de son correspondant et de sa possession d'une clé de chiffrement. Par ailleurs, quel algorithme choisir ? La police belge utilise « PGP » mais d'autres utilisent des algorithmes différents ...

III. Droit international conventionnel en matière de coopération

10. La coopération entre les services de répression de différents États peut se dérouler aussi bien par le recours aux dispositifs et structures d'entraide judiciaire tels qu'Interpol, que par la fourniture directe aux autorités d'un autre État des informations pouvant leur être utiles. C'est notamment le cas de la Belgique qui a signé mais pas encore ratifié la convention de Budapest (pour des raisons techniques et d'instabilité de la politique intérieure).

En règle générale, la coopération internationale entre les services de police suppose le consentement préalable des autorités des États intéressés. Suivant les relations entre les États, la nature des informations en question ou d'autres facteurs, elle peut aussi requérir la conclusion d'un accord international précisant les services participants et les procédures à appliquer.

11. Interpol¹⁶, qui œuvre dans le domaine de la coopération policière, a été la première organisation internationale à organiser une structure d'assistance mutuelle.

Interpol regroupe actuellement environ 186 États, dont les pays pilotes du Programme que sont l'Égypte, la Jordanie, le Liban, le Maroc et le Yémen.

12. Interpol a mis sur pied une structure de coopération particulière : le « *National Central Reference Point System* » (NCRP). Dans chaque État membre d'Interpol qui en fait partie (111 à l'heure actuelle), un bureau central national est le point de contact pour les administrations étrangères aux prises avec des enquêtes menées hors territoire.

La coopération au sein de ce réseau est fondée sur les mêmes principes qui s'appliquent en général à la coopération dans le cadre d'Interpol. Cela signifie que les mesures impliquant le recours à des moyens de coercition (dans le but, par exemple, de préserver des preuves) ne sont normalement pas traitées par ce canal.

13. Une difficulté semble résider dans le fait que les États-Unis utilisent peu Interpol, lui préférant les rapports bilatéraux ...

¹⁴ Décision-cadre 2004/68/JAI du Conseil du 22 décembre 2003 relative à la lutte contre l'exploitation sexuelle des enfants et la pédopornographie, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004F0068:FR:NOT>

¹⁵ <http://conventions.coe.int/Treaty/fr/Treaties/Html/185.htm>.

¹⁶ <http://www.interpol.int>; <http://www.interpol.int/Public/TechnologyCrime/default.asp>

Ce réseau présente, en outre, la difficulté complémentaire de ne pas être spécialisé et d'être parfois décevant : le point de contact belge nous ayant par exemple indiqué avoir une fois contacté le point de contact italien et être tombé sur quelqu'un qui ne parlait qu'italien

14. Le G8 s'est le premier penché sur la problématique de la coopération internationale dans la lutte contre la cybercriminalité.

A l'occasion d'une réunion qui s'est tenue à Washington DC les 9 et 10 décembre 1997¹⁷, les ministres de la justice et des affaires intérieures du G8 ont adopté les principes fondateurs d'un réseau de points de contact nationaux. À ces principes a été ajouté un plan d'action pour la mise en place d'un réseau et un compte-rendu des engagements pris par chaque État adhérent au réseau.

Le réseau a été mis en place, sur base du modèle Interpol, pendant la période allant de 1998 à 2000 et les efforts se poursuivent pour accroître le nombre de pays participants (le réseau comporte actuellement plus de 50 membres).

15. Ce réseau de points de contact se distinguait du NCRP d'Interpol par le fait que cette structure est capable de répondre 24h/24 et 7j/7 aux demandes d'aide qui lui sont adressées. Il s'agit donc d'une structure remarquable par sa rapidité de réponse.

Il est toutefois tout à fait réalisable de rendre opérationnels vingt-quatre heures sur vingt-quatre les points de contact qui font partie du réseau d'Interpol. Par une recommandation du 25 juin 2001, le Conseil de l'Union européenne a d'ailleurs incité les pays qui n'étaient pas membres du G8 à adhérer à ce réseau¹⁸.

Un autre avantage non négligeable est le fait que ces points de contact sont spécialisés en matière d'enquêtes informatiques et capable d'initier les procédures nécessaires pour préserver et obtenir une preuve informatique.

L'idée fondamentale qui sous-tend la création du réseau du G8 est qu'il y a lieu de traiter rapidement et de manière hautement qualifiée les différents types de criminalité liée à la haute technologie. L'accent est mis sur la préservation des preuves dans des milieux où les informations peuvent se perdre ou être détruites rapidement.

Le réseau d'information du G8 est ouvert aux adhésions des pays non-membres.

En faire partie présente l'avantage d'être tenu informé des ordres du jour et décisions d'un club d'*happy few*.

16. La Convention des Nations Unies contre la criminalité transnationale organisée¹⁹, signée à Palerme en 2000, a pour but premier de promouvoir la coopération entre les Etats. Elle trouve donc notamment à s'appliquer dans le cadre de la lutte contre la cybercriminalité.

Elle prévoit des modalités de coopération internationale, en matière d'entraide judiciaire ainsi qu'en matière de confiscation, et invite les Etats à conclure d'autres accords afin de renforcer cette

¹⁷http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/Points%20of%20Contact/24%208%20Communique_en.pdf

¹⁸ Recommandation du Conseil du 25 juin 2001, concernant les points de contact assurant un service vingt-quatre heures sur vingt-quatre pour lutter contre la criminalité liée à la haute technologie (2001/C187/02), J.O.C.E., 03.07.2001.

¹⁹ Disponible sur le site : http://www.uncjin.org/Documents/Conventions/dcatoc/final_documents_2/convention_french.pdf.

coopération.

17. La résolution de l'Assemblée générale des Nations Unies relative à la lutte contre l'exploitation des technologies de l'information à des fins criminelles²⁰ exhorte les Etats membres à coordonner l'action de leurs services de répression, à échanger des informations concernant les problèmes qu'ils rencontrent dans la lutte contre l'exploitation des technologies de l'information à des fins criminelles. Elle poursuit en constatant que les régimes d'entraide judiciaire devraient permettre d'ouvrir rapidement une enquête sur les affaires d'exploitation des technologies de l'information à des fins criminelles et de rassembler et échanger rapidement les éléments de preuve relatifs à ces affaires. L'Assemblée générale a réaffirmé l'importance de ces principes dans une résolution adoptée l'année suivante²¹.

18. L'Agenda de Tunis²², pris lors du Sommet mondial sur la société de l'information, sous l'égide des Nations-Unies, a souligné « *combien il est important de poursuivre les auteurs de cyberdélits, y compris ceux commis dans un pays mais dont les conséquences sont ressenties dans un autre pays. Nous insistons en outre sur la nécessité de disposer d'instruments et de mécanismes efficaces, aux niveaux national et international, pour promouvoir la coopération internationale notamment entre les services de police et de justice dans le domaine de la cybercriminalité. Nous exhortons les Etats à élaborer, en collaboration avec les autres parties prenantes, la législation nécessaire permettant d'enquêter sur la cybercriminalité et de poursuivre en justice les auteurs de cyberdélits, en tenant compte des cadres existants* »²³.

19. La Convention de Budapest contre la cybercriminalité, comme nous venons de le voir, contient des dispositions spécifiques pour développer la coopération internationale.

Elle prévoit les modalités de l'extradition, de l'entraide, qui doit être la plus large possible, et va jusqu'à l'information spontanée.

20. **Le mécanisme d'entraide en matière de mesures provisoires** qu'elle contient va permettre de résoudre en grande partie des difficultés que nous dénonçons. En effet, une Partie peut demander à une autre Partie d'ordonner ou d'imposer d'une autre façon la conservation rapide de données stockées au moyen d'un système informatique se trouvant sur le territoire de cette autre Partie, et au sujet desquelles la Partie requérante a l'intention de soumettre une demande d'entraide en vue de la perquisition ou de l'accès par un moyen similaire, de la saisie ou de l'obtention par un moyen similaire, ou de la divulgation desdites données.

Cette disposition est évidemment capitale, car elle rend plus acceptable le long délai de mise en place nécessaire aux commissions rogatoires.

21. **L'accès transfrontière à des données stockées** est par ailleurs facilité puisqu'une Partie peut, sans l'autorisation d'une autre Partie :

- a. accéder à des données informatiques stockées accessibles au public (source ouverte), quelle que soit la localisation géographique de ces données; ou

²⁰ Résolution 55/63 de l'Assemblée générale des Nations Unies, adoptée le 4 décembre 2000, disponible sur le site : <http://www.cybersecuritycooperation.org/moredocuments/International%20Agreements/55-63%20French.pdf>.

²¹ Résolution 56/121 de l'Assemblée générale des Nations Unies relative à la lutte contre l'exploitation des technologies de l'information à des fins criminelles, adoptée le 19 décembre 2001, disponible sur le site http://www.unodc.org/pdf/crime/a_res_56/121f.pdf.

²² Agenda de Tunis, adopté le 15 novembre 2005, disponible sur le site : http://portal.unesco.org/ci/fr/files/20687/11327544873tunis_agenda_fr.pdf/tunis_agenda_fr.pdf.

²³ Agenda de Tunis, adopté le 15 novembre 2005, point 40, disponible sur le site : http://portal.unesco.org/ci/fr/files/20687/11327544873tunis_agenda_fr.pdf/tunis_agenda_fr.pdf.

- b. accéder à, ou recevoir au moyen d'un système informatique situé sur son territoire, des données informatiques stockées situées dans un autre État, si la Partie obtient le consentement légal et volontaire de la personne légalement autorisée à lui divulguer ces données au moyen de ce système informatique.

22. La loi belge du 28 novembre 2000 sur la criminalité informatique²⁴ a franchi un pas de plus en permettant, dans des hypothèses limitées, de réaliser des perquisitions informatiques s'étendant à l'étranger, moyennant seule information a posteriori des autorités étrangères (Art. 88 ter CIC).

Cette loi ne vise aucunement à octroyer unilatéralement la compétence aux instances judiciaires afin qu'elles se procurent un accès illimité aux données enregistrées à l'étranger. Même si le droit public international ne donne, à l'heure actuelle, aucune interprétation précise quant à l'importance que peut avoir le concept de souveraineté dans le « cyberspace », les principes de droit public international sont conservés dans leur intégralité. Aucune compétence visant à violer intentionnellement la souveraineté d'un autre État n'a été créée.

Cette loi s'applique aux recherches effectuées dans un système informatique au cours desquelles les enquêteurs aboutissent à des données stockées à l'étranger. Il est possible que les enquêteurs ignorent l'origine étrangère de ces données ou encore qu'ils ne parviennent pas à en localiser l'origine avec exactitude. La loi belge décide que l'importance de la vérité dans des cas de grande criminalité justifie que de telles recherches soient menées à l'étranger exceptionnellement.

Lorsque les données concernées se trouvent hors de Belgique, celles-ci ne peuvent être que copiées et non bloquées, la seule finalité de cette compétence extraordinaire étant d'empêcher la disparition d'éléments de preuve.

Lorsque l'origine des données peut raisonnablement être déterminée, l'Etat étranger concerné doit alors être informé par le ministère de la Justice, afin de lui permettre de vérifier si une infraction a été commise ou non.

Le but de cette loi belge est donc de permettre l'utilisation en justice de données recueillies à l'étranger par hasard ou involontairement. En effet, le bien-fondé de l'action pénale menée par les autorités ne peut en principe pas être mis en doute et il n'y a donc aucune raison d'exclure a priori les données recueillies de la sorte comme éléments de preuve.

Cette loi exige toutefois que plusieurs conditions soient réunies pour permettre cette extension :

- elle doit être nécessaire,
- elle ne peut être mise en œuvre que dans le cadre d'une affaire déjà en phase d'instruction,
- la mise en place d'autres mesures plus habituelles serait disproportionnée,
- ou il existe un risque que, sans cette extension, des éléments de preuve soient perdus,
- elle ne peut pas dépasser les niveaux d'accès préalablement définis.

Une controverse existe quant à l'admissibilité de ce type de législation nationale²⁵.

Selon un premier point de vue, le droit international n'interdit pas ce type d'opération, car les données sont techniquement accessibles et disponibles à partir de l'État effectuant la recherche, sans l'aide ni l'intervention de l'État où la recherche a lieu. Du fait que les données présentes n'importe où sur un réseau peuvent être considérées comme ubiquitaires, le fait d'y accéder à partir de l'État où elles ne se

²⁴ *M.B.*, 3 février 2001, <http://www.moniteur.be>.

²⁵ Dixième Congrès des Nations Unies pour la prévention du crime et le traitement des délinquants Vienne, 10-17 avril 2000, Document de base pour l'Atelier consacré au thème "Délits liés à l'utilisation du réseau informatique", A/CONF.187/10, disponible sur le site <http://www.uncjin.org/Documents/congr10/10f.pdf>. Le Conseil d'Etat belge avait par ailleurs exprimé de sérieux doutes sur la légalité de cette perquisition transfrontière jugée contraire au principe de la souveraineté nationale.

trouvent pas effectivement serait une question de droit purement interne et non de droit international. De ce point de vue, il ne serait nécessaire de faire intervenir l'État visé par la recherche à aucun moment. La question de savoir dans quelle mesure des données sont ou non ubiquitaires (par exemple, quand des personnes effectuant des recherches doivent user de différents moyens pour télécharger les données d'un État à un autre) n'est pas encore clairement résolue dans le droit international.

Dans l'autre thèse, selon laquelle toute ingérence dans un réseau informatique situé sur le territoire d'un autre État constitue une violation de la souveraineté territoriale de cet État, deux positions méritent d'être examinées.

L'une veut que les États ne devraient pas être autorisés à rechercher ou à copier des données ni à s'ingérer de toute autre manière dans des systèmes informatiques situés dans un autre État unilatéralement, tout comme il ne serait pas permis qu'ils le fassent en étant physiquement et unilatéralement présents dans cet État. Pour obtenir des éléments de preuve auprès d'un autre État, on devrait suivre les procédures d'entraide judiciaire en place. Cette position est certes conforme aux principes traditionnels, mais elle ne tient peut-être pas compte des difficultés pratiques que posent les enquêtes sur les délits informatiques. Sans doute, les mécanismes de coopération et d'entraide judiciaire et policière renforcés mis en place par le Conseil de l'Europe et par l'Union européenne permettent toutefois d'espérer une meilleure efficacité des recherches, plus appropriée aux risques nouveaux créés par un cyberspace sans frontières.

Pour la seconde, plus pragmatique, le droit international ne fournit actuellement aucune réponse claire aux questions de violation de la législation nationale ou de la souveraineté nationale. Ses partisans estiment que le droit international en la matière pourrait être développé en décidant d'un commun accord au niveau international d'autoriser ces activités en définissant clairement dans quelles conditions les autoriser. Cette solution prévoirait en particulier l'envoi d'une notification à l'État faisant l'objet de la recherche.

Il est, en tout Etat de cause, indubitable que les recherches effectuées de la sorte en dehors des frontières doivent rester exceptionnelles. Si le temps et les connaissances le permettent, et à défaut de solutions alternatives adéquates sur le plan juridique à l'heure actuelle, il convient de suivre la procédure classique des commissions rogatoires internationales.

23. Aux termes de l'article 35 de la Convention de Budapest, chaque Partie désigne un **point de contact joignable 24h/24 et 7j/7**, afin d'assurer la fourniture d'une assistance immédiate pour des investigations concernant les infractions pénales liées à des systèmes et données informatiques ou pour recueillir les preuves sous forme électronique d'une infraction pénale.

Chaque Partie fera en sorte de disposer d'un personnel formé et équipé en vue de faciliter le fonctionnement du réseau.

Le futur point de contact belge insiste sur le fait qu'il ne suffit pas d'avoir une police formée, il faut encore que les magistrats le soient. Aussi, la *Federal Computer Crime Unit* participe-t-elle à la formation technique initiale et continuée des magistrats belges.

Cet article 35 est basé sur l'expérience du sous-groupe du G8 sur le crime de pointe qui a établi un réseau de tels points de contact, comme mentionné ci-dessus.

Afin d'éviter une prolifération des réseaux, il a été convenu que les points de contact du G8 et ceux établis sous la convention sur la cybercriminalité soient fusionnés dans un annuaire simple des points de contact qui seront maintenus par le sous-groupe du G8 sur le crime de pointe et le Conseil de l'Europe.

Cet annuaire est limité à l'utilisation des buts de police.

24. D'autres instruments du Conseil de l'Europe, relevant en matière de coopération internationale en matière pénale en général, sont également ouverts aux signatures des Etats non-membres : la convention européenne d'entraide judiciaire en matière pénale²⁶ et ses deux protocoles additionnels²⁷, ainsi que la convention européenne d'extradition²⁸.

25. Pour le cadre de l'Union européenne, de nombreuses avancées ont été réalisées. Elles peuvent servir de source d'inspiration à d'autres initiatives internationales :

- Une décision du Conseil incite les Etats membres à intensifier et optimiser la coopération policière internationale en vue de la lutte contre la pédopornographie sur internet²⁹.
- Conseil relative aux attaques visant les systèmes d'information³⁰, déjà citée, étend les compétences des juridictions de chaque Etat membre, en particulier même lorsque l'infraction est commise à partir d'un site situé en dehors du territoire ou vise un système localisé sur le territoire national. Enfin, la décision précise les devoirs de coopération des autorités policières et judiciaires en la matière et prévoit également la création de points de contact accessibles 24h/24 et 7j/7 en vue de lutter contre les attaques visant les systèmes d'information.
- Une convention relative à l'entraide judiciaire en matière pénale entre les Etats membres de l'Union européenne a également été prise³¹.
- Une proposition de décision-cadre³² vise également à renverser les règles actuelles en matière de transmission de données, en introduisant le principe de « disponibilité ». Selon ce principe, un Etat membre devra accéder à une demande d'information formulée par un autre Etat, à moins que l'on ne se trouve dans le cadre de l'une des exceptions.
- Les ministres européens de la Justice se sont mis d'accord le 13 juin 2007 à Luxembourg³³ pour mettre en commun le contenu de leurs casiers judiciaires afin de permettre un meilleur échange d'informations sur les condamnations prononcées envers d'éventuels suspects.

²⁶ Signée à Strasbourg le 20 avril 1959, disponible sur le site : <http://conventions.coe.int/Treaty/fr/Treaties/Html/030.htm>

²⁷ Protocole additionnel à la convention européenne d'entraide judiciaire en matière pénale, signé à Strasbourg le 17 mars 1978, disponible sur le site : <http://conventions.coe.int/treaty/fr/Treaties/Html/099.htm>, et deuxième protocole additionnel à la convention européenne judiciaire d'entraide en matière pénale, signé à Strasbourg le 8 novembre 2001, disponible sur le site : <http://conventions.coe.int/Treaty/FR/Treaties/Html/182.htm>

²⁸ Signée à Paris le 13 décembre 1957, disponible sur le site : <http://conventions.coe.int/Treaty/fr/Treaties/Html/024.htm>

²⁹ Décision du Conseil du 29 mai 2000 relative à la lutte contre la pédopornographie sur l'Internet (2000/375/JAI), *J.O.C.E.*, 9 juin 2000, L138/1.

³⁰ Décision-cadre 2005/222/JAI du Conseil, du 24 février 2005, relative aux attaques visant les systèmes d'information, *J.O.U.E.*, 16 mars 2005, L69.

³¹ Convention relative à l'entraide judiciaire en matière pénale entre les Etats membres de l'Union européenne, *J.O.U.E.*, 12 juillet 2000, C 197.

³² Proposition de décision-cadre du Conseil du 12 octobre 2005 relative à l'échange d'informations en vertu du principe de disponibilité, consultable sur le site <http://eur-lex.europa.eu>.

³³ Proposition de décision-cadre du Conseil du 22 décembre 2005 relative à l'organisation et au contenu des échanges d'informations extraites du casier judiciaire entre les Etats membres, <http://eur-lex.europa.eu>. Elle vise à remplacer la décision 2005/876/JAI du Conseil du 21 novembre 2005 relative à l'échange d'informations extraites du casier judiciaire, qui n'apportait qu'une réponse partielle aux dysfonctionnements en matière d'échange d'information.

Cette décision-cadre oblige tous les pays européens à communiquer le plus rapidement possible à l'Etat membre concerné les condamnations qui auront été prononcées envers un de ses nationaux.

IV. Exemples de coopération internationale :

26. De nombreux exemples couronnés de succès peuvent être mentionnés. Citons ainsi la lutte contre la pédopornographie sur internet. Plusieurs opérations de polices coordonnées dans différents pays ont eu lieu ces dernières années, aboutissant à des arrestations :

- a. En avril 2005, l'opération Falcon, menée conjointement par le FBI, la police fédérale américaine, Interpol et la police française, a permis de démanteler un réseau actif dans plusieurs pays européens.
- b. L'opération Icebreaker, menée par Europol le 14 juin 2005, a abouti à une vague de perquisitions dans treize pays européens (Autriche, Belgique, France, Allemagne, Hongrie, Islande, Italie, Pays-Bas, Pologne, Portugal, Slovaquie, Suède, Grande-Bretagne), avec des arrestations en France, Belgique, Hongrie, Islande et Suède.
- c. L'opération Odyseus, réalisée le 26 février 2004 à l'initiative d'Europol, a engendré des actions policières dans 10 pays (Australie, Belgique, Canada, Allemagne, Pays-Bas, Norvège, Pérou, Espagne, Suède, Royaume-Uni).

V. Droits fondamentaux

27. Tous ces efforts pour renforcer la coopération internationale en matière de lutte contre la criminalité ne doivent pas engendrer de dérives sécuritaires, mettant en péril des acquis aussi précieux que la liberté d'expression et le droit au respect de la vie privée. Selon la belle formule de Benjamin FRANKLIN, « *ceux qui abandonnent une liberté essentielle pour obtenir une sécurité temporaire minime ne méritent ni liberté ni sécurité* »³⁴.

En d'autres termes, il doit être tenu compte du principe de proportionnalité, par rapport à la nature et aux circonstances de l'infraction. Des standards communs ou des garanties minimums doivent également être prévues.

28. Cette préoccupation est rappelée dans de nombreux instruments internationaux :

- a. L'Agenda de Tunis³⁵, pris lors du Sommet mondial sur la société de l'information, sous l'égide des Nations Unies, rappelle l'importance du respect des libertés fondamentales : « *les mesures prises pour garantir la stabilité et la sécurité de l'Internet et pour lutter contre la cybercriminalité et le spam doivent respecter la vie privée et la liberté d'expression, conformément aux dispositions qui figurent dans les parties pertinentes de la Déclaration universelle des droits de l'homme et de la Déclaration de principes de Genève* »³⁶.

³⁴ Benjamin FRANKLIN, *Historical Review of Pennsylvania*, 1759.

³⁵ Agenda de Tunis, adopté le 15 novembre 2005, disponible sur le site : http://portal.unesco.org/ci/fr/files/20687/11327544873tunis_agenda_fr.pdf/tunis_agenda_fr.pdf.

³⁶ Agenda de Tunis, point 42.

- b. La Convention de Budapest, dans son préambule et son article 15, rappelle qu'il faut garder à l'esprit la nécessité de garantir un équilibre adéquat entre les intérêts de l'action répressive et le respect des droits de l'homme fondamentaux garantis, entre autres, par le pacte international de 1966 relatif aux droits civils et politiques des Nations-Unies.
- c. Un bon exemple de compromis entre l'efficacité de l'action policière et le respect des droits fondamentaux peut être trouvé dans le Système d'information Schengen (SIS).

Le SIS, réseau informatique composé d'une section centrale à Strasbourg et de sections nationales dans chacun des Etats Schengen, est une vaste banque de données dans laquelle sont intégrées les coordonnées des personnes dont l'extradition est demandée ou auxquelles l'accès à un territoire est interdit ou qui sont déclarées disparues ou qui sont recherchées, à quelque titre que ce soit, dans le cadre d'une procédure judiciaire, ces informations étant fournies par les autorités policières et judiciaires de chaque pays. Le SIS ne peut être interrogé que lors de contrôles frontaliers, de police et de douanes, délivrance de visa ou de titres de séjour³⁷.

Lors de la mise en place de ce système, les dérives possibles n'ont pas échappé au législateur européen, qui a intégré à la Convention instaurant le SIS l'obligation pour les Etats qui y adhéraient de garantir dans leur droit national la protection des données à caractère personnel³⁸. Un seuil minimal de protection a été imposé, celui de la Convention du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.

Mieux, une autorité de contrôle commune a été chargée du contrôle de la fonction de support technique du Système d'information Schengen. Le contrôle est exercé conformément aux dispositions de la présente Convention, de la Convention du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel en tenant compte de la Recommandation R(87) 15 du 17 septembre 1987 du Comité des Ministres du Conseil de l'Europe visant à réglementer l'utilisation des données à caractère personnel dans le secteur de la police et conformément au droit national de la Partie Contractante responsable de la fonction de support technique. L'autorité de contrôle commune est également compétente pour analyser les difficultés d'application ou d'interprétation pouvant survenir lors de l'exploitation du Système d'Information Schengen, pour étudier les difficultés pouvant se poser lors de l'exercice du contrôle indépendant effectué par les autorités de contrôle nationales des Parties Contractantes ou à l'occasion de l'exercice du droit d'accès au système, ainsi que pour élaborer des propositions harmonisées en vue de trouver des solutions communes aux problèmes existants.

29. Cela étant, le respect des droits fondamentaux de la personne ne doit pas seulement être envisagé dans le chef des personnes poursuivies. En effet, par exemple, le droit à la dignité de la victime de pédopornographie s'oppose à ce que des images où elle figure soient inutilement visionnées, fût-ce par les autorités policières. Différentes initiatives ont donc été prises dans ce domaine :

³⁷ Suite à l'élargissement de l'UE à 10 nouveaux Etats membres en 2004, un nouveau système d'informations Schengen (SIS II) est actuellement en cours de développement. Il est question que ce système de 2^e génération comprenne des données biométriques (photographies et empreintes digitales) et permette la mise en relation de signalements.

³⁸ Articles 12, 115, 117, 126 Convention d'application de l'Accord de Schengen du 14 juin 1985, conclue le 19 juin 1990, entre les gouvernements des États de l'Union économique Benelux, de la République fédérale d'Allemagne et de la République française relatif à la suppression graduelle des contrôles aux frontières communes.

- a. Le Child Exploitation Tracking System (CETS), système informatique mis au point par Microsoft et la police canadienne, facilite la lutte contre la pédopornographie en permettant de recouper les informations détenues par les services de police, qui sont souvent noyées dans la masse. Le CETS est une base de données sécurisée, capable de fonctionner avec divers systèmes d'exploitation et utilisant des normes ouvertes. Ce système, désormais également utilisé par l'Italie, permet par exemple de vérifier si une image a déjà été signalée comme ayant un contenu pédopornographique, sur simple base de ses caractéristiques (nombre de pixels etc.) sans qu'il ne soit nécessaire de la visionner, ce qui respecte la victime et rend plus efficace la recherche par son automatisation.
- b. Interpol a créé une Banque d'images d'Interpol sur les abus pédosexuels (BIIAP) aux fonctionnalités similaires accessible à toutes les forces de l'ordre sur laquelle figurent les enfants ayant été identifiés sur des sites pédopornographique. Cette base de données fournit à la personne qui la consulte les informations quant à l'Etat dont relève cet enfant et les coordonnées des services de police compétents, tout en respectant son anonymat. Par ailleurs, une indication précieuse de l'âge de l'enfant pourrait ainsi être trouvée afin d'établir un des éléments essentiels de l'infraction. L'effectivité des poursuites et le respect de la dignité de l'enfant sont ainsi conciliés.

VI. Conclusions

30. On le voit, la coopération internationale s'impose, encore plus qu'auparavant, afin de lutter contre la cybercriminalité et ses particularités.

Celle-ci passera par un travail préalable d'harmonisation des législations mais aussi des technologies.

La technique des réseaux de points de contacts, disponibles à tout moment et spécialisés, semble être une des voies les plus empruntées actuellement. Si on y ajoute le mécanisme des mesures provisoires, on aboutit à une coopération internationale efficace, répondant aux nouveaux défis que lance la cybercriminalité, sans déroger à la souveraineté territoriale des Etats.

L'accès transfrontière aux données est aussi une nécessité qui fera encore l'objet de débats juridiques passionnés et passionnants.

31. Nous devons néanmoins être prudents : certes la cybercriminalité doit être combattue mais pas à n'importe quel prix, pas, en tout cas, au prix de nos libertés fondamentales : tous les actes internationaux le rappellent.

Jean-François HENROTTE³⁹

jf.henrotte@elegis.be

www.elegis.be

mis à jour le 1/02/08

³⁹ Avec la collaboration de Me Fanny COTON, sans qui la rédaction de cette contribution, dans le délai aussi bref qui nous a été donné, n'aurait pas été possible. Notre gratitude va également au doyen Yves POULLET pour sa lecture et ses judicieuses observations.