Nations Unies A/CONF.187/10

Dixième Congrès des Nations Unies pour la prévention du crime et le traitement des délinquants

Vienne, 10-17 avril 2000

Distr.: Générale
3 février 2000

Français
Original: Anglais

Point 5 de l'ordre du jour provisoire*
Prévention efficace de la criminalité: comment suivre le rythme des innovations

Délits liés à l'utilisation du réseau informatique

Document de base pour l'Atelier consacré au thème "Délits liés à l'utilisation du réseau informatique"

Résumé

Pour prévenir et combattre efficacement la criminalité informatique, une action mondiale coordonnée s'impose à différents niveaux. Au niveau national, les enquêtes en la matière requièrent des effectifs, des compétences et des procédures appropriés. Les États sont encouragés à envisager de mettre en place des mécanismes qui permettent d'obtenir dans les délais voulus, à partir de systèmes et de réseaux informatiques, des données précises au cas où celles-ci devraient être produites à titre d'éléments de preuve dans une procédure judiciaire. Au niveau international, les enquêtes appellent des mesures opportunes, qui viendraient s'appuyer sur la concertation entre les services nationaux de répression et des lois idoines.

En complément des initiatives déjà prises à l'échelle internationale, le présent document présente une analyse des moyens propres à faciliter l'échange de connaissances techniques et scientifiques entre services nationaux de répression, mettant en lumière la nécessité de débattre au niveau international des mesures juridiques actuelles et à venir touchant la coopération internationale dans le cadre des enquêtes menées sur la criminalité informatique.

*A/CONF.187/1.

V.99-90955

Table des matières

I. Mandats

1. Par sa résolution 52/91 du 12 décembre 1997, l'Assemblée générale a décidé qu'un des quatre ateliers devant se tenir dans le cadre du dixième Congrès des Nations Unies pour la prévention du crime et le traitement des délinquants aurait pour thème les délits liés à l'utilisation du réseau informatique. Par sa résolution 53/110 du 9 décembre 1998, elle a approuvé le programme de travail du dixième Congrès, notamment l'organisation de quatre ateliers techniques de caractère pratique, dont un consacré à l'examen de la question des délits liés à l'utilisation du réseau informatique. Dans cette même résolution, l'Assemblée a souligné l'importance des ateliers et invité les États Membres, les organisations non gouvernementales et les autres organes et organismes compétents à appuyer les préparatifs de ces ateliers sur les plans financier, organisationnel et technique, y compris l'élaboration et la diffusion des documents de base pertinents.

2. Par sa résolution 54/125 du 17 décembre 1999, l'Assemblée générale a encouragé les États, les autres entités intéressées et le Secrétaire général à collaborer pour faire en sorte que les quatre ateliers soient clairement orientés sur les thèmes abordés et débouchent sur des résultats concrets, et invité les gouvernements intéressés à donner suite à ces ateliers au moyen de projets ou d'activités pratiques de coopération technique. Suite à cette résolution, l'Institut pour la prévention du crime et le traitement des délinquants en Asie et en Extrême-Orient a organisé deux réunions d'experts sur les délits liés à l'utilisation du réseau informatique, au cours desquelles la plupart des préparatifs de fond de l'atelier consacré à ce thème ont été arrêtés. Le Centre pour la prévention internationale du crime se félicite des mesures prises par l'Institut et le groupe d'experts pour permettre la tenue de l'atelier.

II. Objectif et portée du présent document

3. Les réseaux informatiques internationaux comme Internet permettent aux utilisateurs de communiquer avec d'autres utilisateurs à travers le monde, d'agir et d'effectuer des transactions ensemble. Comme l'utilisation d'ordinateurs et de réseaux à des fins légitimes peut s'accompagner d'une utilisation à des fins illégales, il est inévitable que parmi ceux qui explorent les moyens d'exploiter ces nouveaux supports figurent des particuliers ou des groupes nourrissant des desseins criminels. La lutte contre la criminalité dans l'environnement informatique international actuel est complexe pour trois raisons majeures:

a) L'acte criminel peut être perpétré dans un environnement électronique. Les enquêtes sur la criminalité informatique, c'est-à-dire sur toute infraction commise dans un réseau électronique, demandent des connaissances, des procédures et des bases juridiques particulières que les services de répression de l'État considéré ne possèdent pas nécessairement;

b) Les réseaux informatiques internationaux comme Internet sont des environnements ouverts qui permettent aux utilisateurs d'agir par-delà les frontières de l'État sur le territoire duquel ils se trouvent. Or, les services de répression en général ne peuvent enquêter qu'à l'intérieur du territoire de leurs États respectifs. C'est pourquoi la lutte contre la criminalité mettant en jeu des réseaux informatiques ouverts appelle une intensification de la coopération internationale;

c) Le caractère ouvert des structures des réseaux informatiques internationaux offre précisément aux utilisateurs la possibilité de choisir, pour opérer, l'environnement juridique qui leur convient le mieux. Les utilisateurs peuvent choisir un pays où certains actes susceptibles d'être exécutés dans un environnement électronique ne sont pas qualifiés d'infractions pénales. Ce pays peut être le théâtre d'activités menées par des particuliers d'autres États dont le droit pénal réprime précisément pareilles activités. L'existence de "paradis informatiques" – États où la réduction ou la prévention de l'usage abusif des réseaux informatiques ne sont pas une priorité ou dans lesquels il n'existe aucune règle de procédure efficace – risque de contrarier la lutte engagée par d'autres pays contre la criminalité informatique.

4. L'analyse qui suit porte sur les moyens à mettre en œuvre pour mener au niveau international une action coordonnée propre à faciliter, renforcer et améliorer les méthodes actuelles de lutte contre la criminalité informatique. Le rôle que l'Organisation des Nations Unies ou d'autres organisations internationales peuvent jouer en l'occurrence revêt un intérêt particulier. Le présent document renferme des informations de base sur l'atelier consacré à la question des délits liés à l'utilisation du réseau informatique.

5. On trouvera ci-après une énumération des types d'infractions susceptibles d'être commises en relation avec les réseaux informatiques internationaux, de même qu'un exposé des raisons pour lesquelles ces infractions doivent retenir l'attention de la communauté internationale et

mobiliser une action conjointe. L'idée est d'aboutir à une conception commune à l'échelle internationale et d'orienter l'élaboration des politiques pénales nationales en la matière.

III. Catégories de délits informatiques

6. Un environnement électronique, au sens où cette expression est employée dans le présent document, s'entend d'un système informatique ou d'un réseau informatique. Certes, il existe encore des systèmes autonomes, mais il est plus courant qu'un ou plusieurs systèmes informatiques, y compris des micro-ordinateurs, soient interconnectés, formant un réseau. Aux fins du présent document, aucune différence n'est établie entre réseaux privés et réseaux publics, ni entre connexions permanentes et connexions non permanentes, et les systèmes de télécommunication, sauf indication contraire, sont rangés dans la même catégorie que les systèmes et les réseaux informatiques.

7. Aujourd'hui, Internet est un exemple type de réseau informatique public. Il a connu une croissance exponentielle ces dix dernières années. Il doit son succès, pour une large part, à l'utilisation de protocoles communs. Tout exploitant de système ou de réseau qui applique ces protocoles peut aisément devenir un maillon du réseau en tant que "fournisseur de services", ou, dans le présent contexte, fournisseur d'accès à Internet. Pour des raisons commerciales et techniques, les fournisseurs de services, dans certains pays, tendent à s'organiser en associations ou sociétés autour de positions communes sur certaines questions.[1] Selon les estimations, plus de 200 millions de personnes utilisent aujourd'hui Internet, dont 112 millions en Amérique du Nord, 47 millions en Europe et 33 millions dans la région de l'Asie et du Pacifique.[2] À la fin de 1995, les utilisateurs n'étaient que 26 millions, dont la majorité résidaient aux États-Unis d'Amérique. On a estimé qu'en 1999, le nombre d'utilisateurs a augmenté de plus de 3 % par mois.

8. Un système informatique a pour fonction principale de traiter des données. Celles-ci sont censées représenter, par convention, des faits, des instructions ou des notions sous une forme propre à être comprise par l'esprit humain ou à faire l'objet d'un traitement automatisé.[3] Les données électroniques sont représentées par des chaînes ou séquences de points magnétiques situés sur un support permanent ou temporaire, ou sous forme de charges électriques lorsqu'elles sont en cours de transfert. Lorsque les données peuvent être identifiées et pilotées par un support déterminé, comme par exemple les données stockées sur un disque souple ou un ensemble de disques souples, elles peuvent, du point de vue juridique, être considérées comme constituant un objet matériel. En général, les données en cours de traitement dans un système informatique ne peuvent plus être identifiées par un qualificatif et pilotées à l'aide de leur support. Les systèmes d'exploitation transfèrent de façon autonome les fichiers de données d'un emplacement physique sur un support à un autre. Dans les réseaux informatiques, le traitement des données décentralisé ne permet pas à ceux qui sont chargés de piloter les données de déterminer la localisation physique de l'ensemble ou d'une partie d'un fichier sans appliquer des mesures spécifiques. Les données de ce type sont pilotées à l'aide d'une opération logique uniquement et non à l'aide d'une manipulation physique. Il est de ce fait difficile, en droit, de considérer les données pures comme un objet matériel.

9. Le cyberdélit s'entend de toute infraction susceptible d'être commise à l'aide d'un système ou d'un réseau informatique, dans un système ou un réseau informatique ou contre un système ou un réseau informatique. En principe, il englobe toute infraction susceptible d'être commise dans un environnement électronique. Dans le présent document, le mot "délit", ou "infraction", s'entend des faits généralement définis comme étant illégaux, ou qui sont susceptibles de se voir conférer le caractère d'infraction pénale dans un proche avenir. Certains actes peuvent être considérés comme constituant une infraction pénale dans un État, et non dans d'autres, mais comme expliqué au paragraphe 13, on est parvenu dans certaines instances internationales à une entente commune sur les comportements en relation avec les systèmes et les réseaux informatiques qu'il conviendrait de qualifier d'infractions pénales. Tel est le point de départ de l'analyse qui suit.

10. Cette analyse traitera des enquêtes pénales sur la cybercriminalité et des poursuites correspondantes. L'expression "services de répression" s'entend des autorités qui, aux termes de la loi, sont chargées de procéder aux enquêtes et d'engager des poursuites. Il existe dans certains États Membres des services spécialisés chargés d'enquêter sur les délits liés à l'utilisation du réseau informatique ou d'apporter leur concours aux enquêtes de ce type. Sur le plan international, l'Organisation internationale de police criminelle (Interpol) a pour mission de coordonner l'enregistrement et la diffusion des informations communiquées par les services de police concernant par exemple les personnes recherchées et les biens volés.

11. En enquêtant sur un cyberdélit, les services de répression d'un État peuvent solliciter la coopération des

autorités d'autres États sous forme d'assistance dans une affaire donnée et en vue de mettre en commun des informations générales sur les organisations criminelles et les affaires pénales en la matière. Au cours d'une enquête donnée, ils peuvent demander à utiliser des données disponibles dans d'autres États. L'étendue de la coopération entre services nationaux de répression est définie par le droit interne de chaque État, de même que par des accords internationaux, dont des accords d'entraide judiciaire.

12. À titre d'exemple courant de dévoiement des réseaux informatiques internationaux, il y a lieu de citer leur utilisation pour transmettre des propos interdits par la loi, offrir des produits illégaux ou encore faire des offres mensongères afin d'obtenir des avantages financiers illégaux. Dans ces cas, Internet est utilisé de la même manière que tout autre instrument ou outil qui pourrait être utilisé pour perpétrer une infraction. Le réseau lui-même constitue l'environnement de l'infraction, plus qu'un élément indispensable à sa commission. Les caractéristiques propres à Internet peuvent amener celui qui entend commettre un délit à l'utiliser plutôt qu'à recourir à un moyen traditionnel: avec Internet, il dispose d'excellents moyens de communication, il peut taire son identité, outre qu'il ne court pas de grands risques d'être poursuivi au pénal devant tel ou tel tribunal compétent. De plus, certains utilisateurs se servent d'Internet pour accéder illégalement à des systèmes connectés afin de perturber leur fonctionnement ou leur contenu. Cette activité a été désignée par l'expression "délit informatique". L'auteur d'un délit informatique se prévaut de connaissances, de compétences ou d'instruments techniques spécifiques pour mener à bien une activité illicite. Les systèmes informatiques peuvent être des cibles faciles en l'absence de règles de sécurité appropriées ou si les utilisateurs ne sont pas conscients des risques encourus. En outre, les éléments qui font d'un système un système convivial tendent d'un autre côté à concourir à son insécurité. Les failles en matière de sécurité présentées par un logiciel d'exploitation au succès confirmé seront souvent connues sur la place publique.

13. Les problèmes liés à la cybercriminalité transnationale ont retenu l'attention des pays concernés, mais n'ont suscité que peu d'intérêt au niveau mondial. Par exemple, l'Organisation des Nations Unies n'a pas encore adopté de texte sur la criminalisation des cyberdélits; les législations nationales peuvent s'appliquer à ces infractions de différentes manières, si tant est qu'elles s'appliquent. Ce phénomène peut s'expliquer en particulier par une faible participation aux communications électroniques internationales, un manque d'expérience en matière de répression et une sous-évaluation des dommages que les délits informatiques peuvent causer à la société. Dans le cas des réseaux informatiques mondiaux, la politique pénale d'un État a des conséquences directes pour la communauté internationale. Les auteurs de cyberdélits peuvent opérer en passant par un État où leurs activités ne sont pas répréhensibles, et ainsi être protégés par la loi de ce pays. Même si un État n'a sur le plan national aucun intérêt particulier à criminaliser certains actes, il peut envisager de le faire de manière à ne pas devenir un paradis informatique et se retrouver isolé sur la scène internationale. La coopération internationale entre les services de répression et les autorités judiciaires des divers États passe par l'harmonisation du droit pénal positif dans le domaine de la lutte contre la cybercriminalité.

14. La cybercriminalité englobe deux catégories de délits:

a) Au sens étroit ("délit informatique"), elle s'entend de tout comportement illégal faisant intervenir des opérations électroniques qui visent la sécurité des systèmes informatiques et des données qu'ils traitent;

b) Dans une acception plus large ("délit lié à l'utilisation du réseau informatique"), elle s'entend de tout fait illégal commis au moyen d'un système ou d'un réseau informatique ou en relation avec un réseau ou un système informatique. Elle englobe notamment la possession, l'offre ou la diffusion illégales d'informations à l'aide d'un système ou d'un réseau informatique.

15. Telle que définie au paragraphe qui précède, la criminalité informatique concerne tous les actes illégaux perpétrés contre la sécurité d'un système ou de données à l'aide d'opérations électroniques. La sécurité des systèmes informatiques et des données se résume en trois principes: assurance de la confidentialité, de l'intégrité ou de la disponibilité des données et des opérations de traitement. Selon la liste de 1985 de l'Organisation de coopération et de développement économiques[4] et la recommandation plus détaillée du Conseil de l'Europe de 1989,[5] les délits d'atteinte à la confidentialité, à l'intégrité ou à la disponibilité des données recouvrent notamment les faits suivants:

a) L'accès non autorisé, c'est-à-dire l'accès sans droit à un système ou un réseau informatique par violation des règles de sécurité;

b) Les dommages affectant des données ou des programmes informatiques, c'est-à-dire l'effacement,

l'endommagement, la détérioration ou la suppression sans droit de données ou de programmes informatiques;

c) Le sabotage informatique, c'est-à-dire l'entrée, l'altération, l'effacement ou la suppression de données ou de programmes informatiques, ou l'ingérence dans des systèmes informatiques, dans l'intention d'entraver le fonctionnement d'un système informatique ou d'un système de télécommunication;

d) L'interception non autorisée, c'est-à-dire l'interception, sans autorisation et par des moyens techniques, de communications à destination, en provenance ou au sein d'un système ou d'un réseau informatique;

e) L'espionnage informatique, c'est-à-dire l'obtention, la divulgation, le transfert ou l'utilisation sans autorisation ni autre justification légale d'un secret commercial, dans l'intention de causer un préjudice économique à la personne ayant droit au secret, ou d'obtenir pour soi-même ou pour autrui un avantage illégal.

16. La première de ces formes de criminalité, à savoir l'accès non autorisé, appelé parfois "piratage", est fréquente et s'accompagne souvent de l'endommagement de données ou d'un acte d'espionnage informatique. Une variante moderne courante est le piratage opéré sur un site Web pour y incorporer des données injurieuses ou préjudiciables. Pour que les enquêtes sur ces délits de piratage soient efficaces, il faut en règle générale que la victime coopère et que l'auteur soit pris sur le fait. Les auteurs sont souvent des jeunes, brillants, vouant une passion à la technique, qui n'ont qu'une faible conscience morale de leurs actes ou des dommages qu'ils pourraient causer. Certains pays ont criminalisé, outre les délits de piratage, certaines activités comme le trafic de mots de passe ou de dispositifs de piratage.

17. L'endommagement de données et de programmes informatiques comprend l'introduction de "vers" ou de "virus" informatiques. Un ver peut finir par entraîner l'interruption totale du fonctionnement de l'ordinateur, tandis qu'un virus peut entraîner l'effacement de toutes les données stockées dans le disque dur. La propagation des virus se fait aujourd'hui par l'expédition des messages électroniques non sollicités. Les utilisateurs d'Internet ne sont pas forcément conscients du risque que présentent les réseaux électroniques ouverts et la réception de messages non sollicités. Pour des raisons financières, il ne sera peut-être pas possible d'utiliser les programmes de détection de virus disponibles sur le marché. Les enquêteurs peuvent avoir du mal à prouver qui est responsable de l'introduction du virus qui a causé les dommages. Les pirates peuvent aussi utiliser à leur profit (temporairement) les failles qui se glissent dans la sécurité des programmes informatiques qui sont fréquemment utilisés et accéder aux systèmes informatiques d'autrui, voire, dans des cas exceptionnels, prendre leur contrôle en y stockant des fonctions spécifiques. Il se peut que les utilisateurs d'Internet ne soient pas dûment au fait des risques éventuels, ni des règles de sécurité supplémentaires offertes par les fabricants de logiciels d'exploitation.

18. La fraude informatique est définie par le Conseil de l'Europe (voir par. 15 ci-dessus) comme:

> "L'entrée, l'altération, l'effacement ou la suppression de données ou de programmes informatiques, ou toute autre ingérence dans un traitement informatique, en causant par là même un préjudice économique ou matériel à une autre personne dans l'intention d'obtenir un avantage économique illégitime pour soi-même ou pour autrui."

Cette définition renvoie au cas où l'auteur de l'infraction s'immisce – avec ou sans droit – dans le bon fonctionnement du traitement informatique des données, avec des conséquences analogues à celles de la fraude. Elle ne vise pas les moyens bien connus utilisés pour tromper autrui à travers des représentations ou communications électroniques via Internet, comme par exemple l'offre à la vente de parts à des prix avantageux; les investissements dans l'immobilier dans un État étranger; les prêts à un taux usuaire; le paiement d'avance de biens décrits vaguement; ou l'encouragement à participer à une opération "pyramide". Il est probable que les dispositions traditionnelles sanctionnant les fraudes s'appliqueront à ces faits.

19. Le faux en informatique est défini comme suit par le Conseil de l'Europe (voir par. 15 ci-dessus):

> "L'entrée, l'altération, l'effacement ou la suppression de données ou de programmes informatiques, ou toute autre ingérence dans un traitement informatique, d'une manière ou dans des conditions qui, d'après le droit national, constitueraient l'infraction de faux s'ils avaient concerné un objet traditionnel de ce type d'infraction."

Le but est de criminaliser le faux en informatique de la même manière que le faux en écritures.

20. Il conviendrait de citer à ce stade deux autres catégories de délits connexes. La première concerne

certaines formes d'escroquerie dans les services de télécommunication. Dans ces cas, l'auteur tente, à travers une manipulation technique des dispositifs ou d'éléments électroniques des dispositifs, d'obtenir un service sans le rémunérer. Ce fait tombe généralement sous le coup de dispositions pénales spécifiques, mais il peut relever aussi des dispositions classiques frappant les délits de fraude ou de faux. La deuxième concerne l'usage impropre d'instruments de paiement. L'auteur, en manipulant ou en contrefaisant une carte bancaire électronique, ou en utilisant de faux codes, tente d'obtenir un avantage financier par des voies illégales. Ce fait peut être assujetti à des dispositions pénales spécifiques ou aux dispositions classiques frappant la fraude et le faux, ou encore, *mutatis mutandis*, à la définition donnée au paragraphe 19 ci-dessus.

21. Les délits assistés par ordinateur englobent le fait de mettre à la disposition certaines données, de les communiquer et de les diffuser, et parfois tout simplement le simple fait d'être en leur possession. Leur commission ne nécessite pas le recours à des réseaux électroniques, mais l'auteur peut utiliser des réseaux électroniques pour multiplier l'effet du délit et essayer de se soustraire à la justice. Pour ce qui est des délits liés au contenu des données, il y a lieu d'établir une distinction entre, d'une part, un contenu illégal du fait de sa nature ou de sa signification, et, d'autre part, un contenu qui n'est pas nécessairement illégal en soi mais qui le devient en raison des circonstances qui entourent sa diffusion. Dans cette dernière catégorie entrent l'atteinte au droit d'auteur et la vente de biens ou de services interdits, par exemple armes, drogues, biens volés, médicaments sans ordonnance et accès à des installations de jeu. L'autre catégorie de délits englobe la diffusion de messages qui sont diffamatoires, qui incitent à la subversion ou à la perpétration d'autres faits illégaux, ou qui sont injurieux en raison de leur caractère discriminatoire à l'égard d'une religion ou d'une race, ou en raison de leur caractère pornographique. L'incrimination de ces faits varie considérablement d'un pays à l'autre. Dans la plupart des cas, ces délits font déjà partie du droit existant, et la question est de savoir si les lois correspondantes s'appliquent à l'environnement électronique.

22. Les positions et les règles à travers le monde convergent pour condamner la diffusion de matériel pornographique impliquant des enfants. Des organisations internationales comme l'Organisation des Nations Unies pour l'éducation, la science et la culture et l'Union européenne ont recommandé aux pays qui ne l'ont pas encore fait de promulguer des lois frappant de peines la distribution de matériel de cette nature. Dans de nombreux États, des lois dans ce sens sont en cours d'élaboration ou ont été promulguées. Les services de police, à l'échelon national et international, ont de leur côté accordé un rang de priorité élevé aux enquêtes sur la pornographie impliquant des enfants.

23. En revanche, s'agissant de l'incitation à la haine ou de la discrimination, leur criminalisation, pour diverses raisons, ne fait pas l'unanimité. Mais il se peut que cette situation change à mesure que la communauté internationale prend conscience des effets préjudiciables de tels comportements.

24. La diffusion de documents illégaux a amené à s'interroger sur le rôle et les responsabilités des fournisseurs d'accès à Internet. Hormis quelques rares initiatives législatives prises pour définir et délimiter leur devoir de vigilance, la tendance, au niveau aussi bien international que national, est à conférer à ces fournisseurs un statut juridique analogue à celui des opérateurs de télécommunications traditionnels. En d'autres termes, les fournisseurs ne sont pas juridiquement tenus de surveiller ou éventuellement de bloquer la circulation de l'information passant par leur système informatique. Il reste qu'un fournisseur d'accès à Internet, en règle générale, est tenu de prendre toutes mesures nécessaires pour empêcher la poursuite de la diffusion d'éléments d'information illégaux une fois au courant de leur nature.[6] D'autres aspects aussi de l'application du droit interne aux fournisseurs d'accès à Internet ne sont peut-être pas suffisamment clairs. Il en est ainsi notamment de l'étendue de la responsabilité civile éventuelle pour la transmission de matériaux illégaux et de l'étendue de l'obligation pour un fournisseur d'accès à Internet de coopérer avec les services de répression en fournissant des informations dans le cadre d'une enquête criminelle donnée ou une autre forme d'assistance.

IV. Enquêtes criminelles sur les cyberdélits

25. Comme indiqué plus haut, un cyberdélit s'entend de toute infraction commise à l'aide de moyens électroniques ou commise, en tout ou en partie, dans un environnement électronique. Ce sont ces infractions que les enquêtes criminelles dans un environnement électronique visent. Néanmoins, d'autres crimes peuvent aussi laisser des traces ou des preuves dans cet environnement. Aussi les enquêtes criminelles ne se limiteront-elles donc pas au cyberdélit au sens du chapitre qui précède; elles engloberont aussi les

enquêtes sur toute infraction à propos de laquelle des éléments de preuve (potentiels) doivent être obtenus dans un environnement électronique.

26. Les enquêtes criminelles dans un environnement électronique nécessitent des compétences techniques et des procédures idoines et doivent être fondées en droit. Les recommandations de 1989 et 1995 du Conseil de l'Europe (R (1989) 9 et R (1995) 13) mettent l'accent sur le fait que les services nationaux de répression doivent constituer des brigades spécialisées dans la criminalité informatique, dûment dotées en effectifs, en matériel et en logiciels et dont les membres bénéficieraient de programmes de formation et de mise à niveau. Maints pays en ont déjà créé. Un certain nombre d'entre eux ont publié des manuels contenant des instructions d'ordre technique, scientifique et procédural sur la manière de mener les enquêtes afin de réduire les disparitions d'éléments de preuve et d'en garantir la recevabilité devant les tribunaux.

27. Dans certains pays, des brigades de la police nationale "patrouillent" sur Internet, et des logiciels spécifiques ont été mis au point pour détecter notamment les délits de piratage ou de diffusion de documents pornographiques impliquant des enfants. L'Union européenne a participé au financement de la mise au point par la police suédoise d'un logiciel pour localiser les documents pornographiques impliquant des enfants (voir http://www.techweb.com). Étant donné l'énorme quantité d'informations disponibles dans les réseaux informatiques internationaux, il semble indispensable de mettre au point des outils logiciels, comme par exemple ceux qui reposent sur la reconnaissance des formes.

28. Il existe deux méthodes pour obtenir des données dans un système informatique, qui sont basées l'une sur des critères techniques et l'autre sur des critères juridiques. Dans le premier cas, les données sont obtenues dans le cadre d'une perquisition dans des locaux ou au lieu où se trouve le système. La seconde méthode concerne l'interception ou la surveillance de données transmises à partir du système, à destination du système ou à l'intérieur du système. Il ne sera pas question ici du pouvoir légal de perquisition des locaux, car il est supposé qu'il englobera celui de perquisitionner dans un système informatique situé dans un lieu donné. L'interception peut être opérée par des moyens techniques extérieurs au système, ou à l'aide de moyens incorporés à cette fin dans le système.

29. Les lois de procédure pénale classiques prévoient généralement la saisie et le blocage de tout le système informatique, comme cela est le cas de n'importe quel autre élément de preuve. Si elles ne le font pas, il ne serait peut-être pas juridiquement possible d'enquêter sur le contenu d'un système informatique contre la volonté de son (ses) propriétaire(s) légitime(s). Il se peut que la saisie de tout un système informatique ne soit pas techniquement possible, ou qu'elle soit disproportionnée du fait de l'existence d'un environnement multiutilisateur ou d'un intérêt mutiutilisateur dans le contenu des données. Il se peut également que les pouvoirs classiques existants ne suffisent pas pour obtenir des informations aux fins d'une enquête donnée, et ce pour les raisons suivantes: a) l'existence de problèmes liés à l'accès au système informatique; b) le fait que les données sont immatérielles; et c) le fait que des données peuvent être stockées dans un système connexe situé à l'extérieur des locaux visés par la perquisition.

30. Si les services de répression trouvent dans les locaux dans lesquels ils perquisitionnent un système informatique, la loi, en général, les autorise à y avoir accès et à inspecter son contenu. Tel est le cas si le système est déjà en marche, si la personne concernée l'ouvre de son gré, ou lorsqu'un moyen d'accès est trouvé dans les locaux mêmes. Si non, la question est de savoir si la loi autorise les services de répression à avoir accès au système contre la volonté de l'intéressé.

31. Les systèmes informatiques, les programmes informatiques ou les fichiers de données peuvent être dotés de dispositifs de sécurité qui les rendent inaccessibles sans autorisation. Leur accès est alors assujetti à des procédures d'identification et d'authentification, c'est-à-dire que l'utilisateur doit donner un mot de passe – manuellement ou à travers une carte à puce, ou selon les deux moyens – ou autoriser la vérification de signes biométriques. En général, la sécurité des données se fait par cryptage, qui permet l'authentification, protège la confidentialité et suppose le recours à un algorithme cryptographique et à une ou plusieurs clefs. Le cryptage présente un risque sérieux, en ce sens que sans l'assistance volontaire de l'opérateur ou de la personne autorisée, le système informatique ou les données recherchées demeureront inaccessibles. C'est pourquoi certaines législations imposent aux opérateurs l'obligation d'autoriser l'accès au système ou aux données, sous peine de poursuites pour résistance en cas de refus. Mais ces lois peuvent ne pas s'appliquer dans les cas où l'opérateur est aussi soupçonné de l'infraction, parce que cela contreviendrait aux règles et principes qui veulent que nul ne peut être tenu de témoigner contre lui-même. Ceux qui ont d'autres raisons juridiques de ne pas coopérer, soit parce qu'ils ont des liens avec le suspect, soit parce qu'ils sont tenus au secret professionnel, peuvent eux aussi être exemptés de cette

obligation. Dans les cas où il n'y a aucune personne présente à qui enjoindre d'apporter son assistance, toute autre personne (en général un expert extérieur) peut être enjointe de le faire. Il se peut que le simple fait de donner accès aux données ne suffise pas si celles-ci sont cryptées. Dans ces cas, la loi peut obliger à décrypter les données.

32. Les données en tant que telles étant immatérielles, les pouvoirs de saisie classiques ne s'y appliquent généralement pas. À l'occasion d'une enquête criminelle, les objets matériels seront soit saisis, soit emportés, ou alors des mesures seront prises pour faire en sorte que nul en dehors des enquêteurs ne puissent en disposer. Avec les données, il suffit en général de faire une copie. D'autres mesures supplémentaires sont cependant requises lorsque les données présentent un risque, sont illégales ou ont une valeur, ou lorsque la possibilité existe qu'il soit porté atteinte aux victimes ou au déroulement de l'enquête. La loi peut alors autoriser les enquêteurs à effacer les données ou à empêcher qu'elles ne soient utilisées plus avant. Pour protéger les données, un juge peut ordonner qu'elles soient copiées pour être rétablies dans leur état original. Si l'intéressé dénonce la reproduction et l'utilisation ultérieure des données, la loi peut exiger la délivrance d'une déclaration officielle faisant état de la récupération des données.

33. La perquisition dans un système informatique se déroulera généralement dans le cadre d'une perquisition opérée dans des locaux ou des lieux, et normalement à l'intérieur de leurs frontières matérielles. Mais il se peut qu'un réseau informatique ne soit pas situé en un lieu unique et qu'il soit connecté à d'autre éléments au moyen de lignes de communication fixes ou établies par commutation. Dans ce cas, il s'agit de savoir si la loi autorise les perquisitions dans les systèmes connectés si ceux-ci ne se trouvent pas dans les locaux faisant l'objet de la perquisition. Or, des données risquent d'être détruites avant la délivrance d'un mandat de perquisition complémentaire visant le lieu où les données se trouvent physiquement. Dans les grands réseaux, il se peut qu'il soit pratiquement impossible de localiser avec précision les données.

34. Le mandat de perquisition complémentaire repose sur les principes juridiques suivants. La personne qui réside dans les locaux devant faire l'objet de la perquisition a le droit d'avoir accès au système informatique connecté et d'utiliser ses fonctions et sa capacité de stockage. Elle peut garder la haute main sur les données en restant sur place. Lors de la perquisition, elle est juridiquement tenue d'autoriser la perquisition dans les locaux qui se trouvent physiquement sous son contrôle. L'on pourrait faire valoir que les mêmes règles devraient s'appliquer aux données auxquelles la personne en question a effectivement accès, même si celles-ci se trouvent peut-être ailleurs. Il s'ensuivrait que la perquisition complémentaire se limiterait aux activités que l'intéressé est autorisé à exercer en rapport avec le système connecté et les données, et qu'elle ne portera pas atteinte à ses droits plus que la perquisition initiale. Il serait possible de limiter ces pouvoirs aux enquêtes portant sur des infractions graves ou aux cas où une action immédiate s'impose pour empêcher la disparition d'éléments de preuve, ou à ces deux cas. D'autres restrictions pourraient être envisagées dans le cas où le système connecté ou les données recherchées relèvent d'une juridiction étrangère (voir le paragraphe 59 ci-après).

35. La recherche et la sélection des données dans un système informatique soulèvent un certain nombre d'autres problèmes juridiques. Le premier consiste à déterminer dans quelle mesure il importe de préciser la nature et la structure des données recherchées pour faire de cette opération une opération légale. Les législations nationales peuvent imposer à cet égard différentes restrictions. Par ailleurs, l'exécution fidèle et précise de l'ordonnance du juge peut prendre très longtemps si les services de répression sont amenés à copier autant de données jugées pertinentes pour l'enquête que possible. Les législations nationales peuvent ou non autoriser pareille pratique. Une autre question importante consiste à savoir si l'intéressé devrait être informé des données qui sont reproduites pour être emportées, dans quelle mesure il devrait l'être et s'il devrait avoir le droit de contester devant les tribunaux la saisie des données. Un autre problème se pose dans le cas des données protégées juridiquement ou d'une autre manière: il s'agit de savoir comment identifier et protéger ces données lorsque les autorités copient de grandes quantités de données pour les examiner ultérieurement.

36. En outre, il est à noter que les données sont volatiles. Elles peuvent être facilement transférées, effacées ou altérées sans laisser de traces bien nettes. Le traitement des données décentralisé n'est pas l'unique facteur qui fait des données des éléments volatiles. Le traitement électronique des données suppose le traitement de grandes quantités de données éphémères susceptibles d'être effacées dès qu'elles ne serviront plus. Tel est le cas par exemple des données figurant dans les fichiers de consignation ou des données de trafic en matière de télécommunication. Si l'ensemble de données "original" (si tant est que cette expression ait un sens dans le contexte du traitement des données) est inconnu, il est difficile de détecter les manipulations, et il sera impossible de rétablir les fichiers

supprimés si des copies de sauvegarde n'ont pas été conservées. En matière de perquisition physique, la nature des données pose des problèmes:

a) La recherche de données stockées dans un support électronique ou en cours de transmission devra dans la plupart des cas être effectuée rapidement et opportunément afin d'éviter toute immixtion dans la perquisition ou toute falsification de données;

b) Des précautions particulières doivent être prises afin que les données puissent être produites devant les tribunaux en tant qu'éléments de preuve. L'intégrité des données doit être assurée dès le moment où celles-ci sont téléchargées ou copiées à partir du système informatique visé par la perquisition jusqu'au moment où elles sont produites devant le tribunal.

37. Les distinctions, du point de vue technique et juridique, entre la saisie de données stockées et l'interception de données en circulation dans le réseau se sont elles aussi estompées. Les données sont traitées à l'aide d'un système informatique, appelé aussi système automatisé de traitement de l'information. Le processus comprend l'entrée des données, leur transfert vers le matériel périphérique (par exemple un écran vidéo) et les supports de stockage temporaire, le traitement en tant que tel, la transmission des résultats vers les unités périphériques pour stockage et la sortie ou la transmission vers d'autres éléments du système. Intercepter des données dans un système informatique revient généralement à rechercher des données stockées, en faisant appel aux fonctions du système ou à des programmes informatiques spécifiques. La recherche de données en cours de transmission peut se faire en utilisant les dispositifs mêmes du système (dispositifs de surveillance), s'ils existent, ou en interceptant par des moyens techniques le flux de données quelque part dans le dispositif de transmission. Étant donné que, dans de nombreux cas, les données sont à la fois stockées et en circulation, ou qu'elles passent fréquemment d'un état à l'autre, il sera souvent loisible aux enquêteurs d'opter, pour obtenir les mêmes données, soit pour la saisie, soit pour l'interception. Cette possibilité risque de soulever des problèmes juridiques car, dans de nombreux États, les normes ou garanties applicables diffèrent selon qu'il s'agit de l'interception de communications ou de la saisie d'informations stockées. L'interception de données en circulation est souvent assujettie à des normes plus strictes parce qu'elle est une opération secrète; elle peut toucher des données qui n'existaient pas au moment où la perquisition a été autorisée ou a débuté; et, dans la plupart des cas, les parties concernées n'auraient connaissance de l'interception et pourraient n'en être informées, si tant est qu'elles le soient, que bien plus tard. Le fait que des données en réseau peuvent être ou saisies ou interceptées risque dans certains cas de porter atteinte aux droits des suspects parce qu'il permettrait aux services de répression d'appliquer à certaines opérations qui relèvent davantage de l'interception les règles juridiques moins restrictives de la saisie.

38. Les données électroniques copiées à partir de fichiers de données ou enregistrées à partir des flux de données appellent généralement des précautions et des mesures spéciales pour pouvoir servir éventuellement d'éléments de preuve devant les tribunaux. Dans plusieurs systèmes juridiques, le principe selon lequel tous les éléments de preuve doivent être produits devant le tribunal exige que ceux-ci soient de très grande qualité. Il peut exister dans certains pays des conditions formelles empêchant ou prévenant la production de données électroniques en tant qu'éléments de preuve. Certaines législations prévoient que les éléments de preuve doivent être communiqués par écrit, afin qu'il puisse en être donné lecture à l'audience, par exemple. Dans certains pays, les données sous forme de sons ou d'images ne répondraient pas à cette condition et ne seraient donc pas recevables. Tout doute quant à la fiabilité des éléments de preuve rendra ceux-ci généralement irrecevables. Dès lors que les données électroniques peuvent aisément être modifiées sans qu'il reste de traces, les services de répression ont pour lourde tâche de recueillir ces données en faisant appel à des procédures transparentes et sûres qui permettent d'établir leur authenticité. Pour s'assurer de l'authenticité des données, le juge doit être à même d'évaluer la fiabilité du processus de reproduction et d'enregistrement des données en remontant au support d'origine. Il doit pouvoir aussi: a) vérifier la validité de la procédure de sauvegarde et la sécurité de la sauvegarde elle-même; b) procéder à une analyse des pièces; et c) s'assurer que les données présentées au tribunal cadrent avec les données saisies et recueillies à l'origine.

39. De nombreux systèmes juridiques nationaux confèrent au juge, outre le pouvoir classique d'ordonner une perquisition dans des locaux, celui d'ordonner la communication d'objets matériels. Dans certains cas, ils peuvent parallèlement l'autoriser à ordonner la communication de données spécifiées, mais cette compétence peut être soumise à des restrictions et à des conditions spécifiques qui ne s'appliquent pas aux pouvoirs classiques en matière d'ordonnance de communication d'informations, et ce afin qu'elle ne puisse être utilisée pour obtenir des informations autres que celles

spécifiées. Si de tels contrôles n'existaient pas, il se pourrait par exemple qu'une ordonnance impose à un individu l'obligation de recueillir, traiter ou sélectionner n'importe quelle autre catégorie de données qui n'est pas stockée et qui ne se trouve pas sous son contrôle. Pareille obligation dépasserait l'étendue et l'objet des ordonnances de communication d'informations. Il peut s'avérer utile que les services de répression demandent que l'ordonnance vise, outre la communication des données recherchées, celle des fichiers de consignation du système informatique, ces fichiers enregistrant dans l'ordre chronologique toutes les transactions effectuées sur le système, avec indication de l'heure, de la durée et des terminaux à partir desquels les données ont été captées ou modifiées.

40. Dans le droit classique de nombreux pays, une autorité judiciaire ou autre peut ordonner l'interception et l'enregistrement consécutif de communications utilisant le réseau public. Certains pays ont élargi ce pouvoir aux réseaux privés, à de nouvelles formes spécifiques de communications, par exemple les communications par systèmes mobiles ou par satellite, et aux réseaux informatiques. L'idée est que si une communication peut être interceptée sur un réseau et pas sur un autre, les criminels utiliseront le réseau à partir duquel les communications auraient le moins de chances d'être interceptées par les services de répression. L'interception légale de communications spécifiées exige des installations techniques particulières, dont la mise en place doit être prévue par la loi, et l'exécution rapide de l'ordonnance d'interception délivrée par le juge.

41. Pour identifier les communications à intercepter et les personnes prenant part à une communication interceptée, il est indispensable de s'assurer la coopération des opérateurs de réseaux, comme les opérateurs de réseaux de télécommunication et les fournisseurs d'accès à Internet. Eux seuls possèdent les renseignements voulus sur leurs clients. Si besoin est, la législation nationale peut imposer aux opérateurs et aux fournisseurs d'accès l'obligation de remettre promptement, sur instruction des autorités compétentes, les coordonnées concernant le client. Des obligations juridiques non équivoques dans ce sens ont d'autre part pour avantage de décharger les particuliers et les sociétés de toute obligation de réparation vis-à-vis de leurs clients.

42. Les opérateurs de réseaux de télécommunication et les fournisseurs d'accès à Internet possèdent normalement des données de trafic concernant les communications passées, établies par un dispositif qui enregistre les détails, y compris l'heure, la durée et la date de toute communication, les coordonnées des correspondants et le type de service ou d'activité (voir l'exemple du fichier de consignation d'un système informatique, au paragraphe 37 ci-dessus). Ces données sont en général conservées pendant une durée limitée, selon les besoins commerciaux de l'opérateur ou du fournisseur d'accès et les critères juridiques (dans l'Union européenne) ou commerciaux régissant la protection de la vie privée. Nombre de législations nationales autorisent les services de répression ou les autorités judiciaires à ordonner la collecte de données de trafic pour des communications à venir. Dans les cas où des données de trafic font partie de la communication, telles que "les données d'en-tête" des messages électroniques, on peut considérer cependant que leur collecte constitue une interception de la communication elle-même et, qu'à ce titre, elle est soumise aux restrictions juridiques applicables. Dans les autres cas, on peut considérer que la collecte de données de trafic sans interception du contenu de la communication elle-même porte moins atteinte à la vie privée des intéressés et qu'elle est donc soumise à des critères juridiques moins contraignants.

43. Les cas de piratage ou d'intrusion électronique mettent en lumière la nécessité d'intercepter rapidement une communication électronique, de disposer promptement des données de trafic et des coordonnés du client de manière à remonter à la source de la communication, à sauvegarder les données et à prendre l'auteur sur le fait, pour des raisons de preuve évidentes. Même s'il constitue une infraction pénale, le piratage, dans certaines législations, n'est pas nécessairement considéré comme une infraction suffisamment grave pour justifier l'adoption des mesures d'interception. De façon générale, un acte de piratage recouvre d'autres faits plus graves que ceux qui peuvent être établis au moment de sa détection. Ce serait là peut-être une autre raison pour autoriser l'interception dans les cas d'intrusion électronique.

44. L'interception d'une communication électronique peut-être gênée par le fait qu'elle est cryptée. Le cryptage sert à garantir l'authenticité d'un message, à identifier son expéditeur et à déterminer son intégrité. Il sert également à garantir la confidentialité du message (en le protégeant des tiers). Des politiques de cryptage éventuelles ont fait l'objet récemment de débats dans un certain nombre d'organisations internationales. Les responsables de la répression et de la lutte contre la criminalité se déclarent préoccupés par les difficultés qu'ils rencontrent pour obtenir un accès légal aux données cryptées, et les tenants de la protection de la vie privée et des intérêts commerciaux défendent le cryptage au nom de la protection des données personnelles et commerciales.

45. Ce débat dépasse, dans sa majeure partie, le cadre du présent document, mais deux questions précises méritent d'être examinées ici. Certains pays qui fabriquent des dispositifs de chiffrement ont envisagé de surveiller la prolifération des systèmes de chiffrement de manière à empêcher des groupes criminels ou terroristes d'y avoir accès, en mettant en place un régime de licence pour les dispositifs suffisamment "puissants" pour que les services de répression aient du mal à avoir accès aux données. Certains pays ont aussi cherché à appliquer des mesures d'ordre pratique pour garantir l'accès en toute légalité aux communications électroniques cryptées. Il s'agit notamment de l'utilisation de puces spéciales, de systèmes qui permettent de confier la garde des clefs de messages à des tiers auprès desquels elles peuvent être en toute légalité récupérées pour avoir accès aux données, ou encore de mesures spéciales qui permettent de décrypter les messages à l'aide de moyens techniques. Ces mesures se sont heurtées à des problèmes d'ordre technique et à l'opposition des défenseurs de la protection de la vie privée et des intérêts commerciaux.

46. L'accès à des communications ou à des données stockées cryptées dans le cadre d'une enquête criminelle intéresse de toute évidence les services de répression du monde entier. Il se peut qu'il existe déjà dans certains pays des mesures permettant de faire face en partie à ce problème. Dans de nombreux cas, les opérateurs de systèmes de télécommunication et de réseaux recourront eux-mêmes au cryptage pour protéger leur propre système et les communications de leurs clients. Dans le cas où ils sont juridiquement tenus de coopérer avec les services de répression aux fins de l'interception d'une communication donnée, il semble raisonnable de supposer que cette obligation englobe, ou pourrait englober, l'obligation de faire sauter tout cryptage qu'ils utiliseraient. Cette obligation ne s'étendrait pas au cryptage utilisé directement par le client, que l'opérateur, normalement, serait incapable de briser. Il existe une autre possibilité: les législateurs des différents pays peuvent envisager d'imposer aux personnes qui prennent part à une communication cryptée l'obligation de fournir les moyens de la décrypter, dans les cas où l'autorité judiciaire compétente l'ordonne. Pour protéger le principe selon lequel nul ne peut être tenu de témoigner contre lui-même, cette obligation pourrait ne pas viser les suspects ou d'autres personnes bénéficiant d'une exemption légale.

47. Comme indiqué au paragraphe 37 ci-dessus, la plupart des pays établissent une distinction entre l'interception de données en circulation et la confiscation de données stockées, mais cette distinction ne vaut pas pour le courrier électronique, parce qu'il combine transfert et stockage de données. Lorsqu'un message est expédié, il est transmis par le prestataire de services de l'expéditeur au prestataire de services du destinataire, lequel à la réception, conserve le message dans la boîte aux lettres du destinataire jusqu'à ce que celui-ci l'ouvre. Le destinataire a accès au message et décide de la durée pendant laquelle il sera conservé dans la boîte aux lettres. Les messages qui s'y trouvent sont ainsi placés sous le contrôle à la fois du destinataire et du fournisseur de services, et les services de répression peuvent normalement y avoir accès en usant du pouvoir de contrainte contre l'un ou l'autre. En règle générale, ils préféreront se retourner contre le fournisseur d'accès à Internet pour ne pas éveiller l'attention du destinataire quant à l'existence d'une enquête. Dans ces conditions, le pouvoir légal d'intercepter une communication et celui de procéder à une perquisition dans des locaux et tout ordinateur qui s'y trouverait peuvent effectivement se confondre. Dans ce sens, la légalité d'une ordonnance exigeant la remise des messages existants et des messages qui arriveraient dans un délai donné serait sujette à caution, à moins que l'ordonnance ne réponde aux critères juridiques (généralement plus rigoureux) régissant l'interception des messages. Vu que les données se trouvent simultanément sous le contrôle du fournisseur de services et du client, on peut se demander, au moment de solliciter l'autorisation légale de procéder à une perquisition ou à une interception, si ce sont la vie privée, les biens ou autres droits et intérêts du premier ou du second qui sont en jeu.

V. Coopération internationale entre les services nationaux de répression

A. Formes de la coopération et des initiatives internationales

48. Étant donné la dimension internationale des réseaux électroniques, il est de moins en moins probable que tous les éléments constitutifs d'un cyberdélit soient confinés à un seul territoire national. Lors des enquêtes, les services de répression de différents États devront coopérer entre eux, aussi bien à titre officiel, en recourant aux dispositifs et structures d'entraide judiciaire tels qu'Interpol, que de manière informelle, en fournissant directement aux autorités d'un autre État des informations pouvant être utiles. 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.

49. En 1997, le Groupe des Huit, composé des chefs d'État ou de gouvernement de sept pays les plus industrialisés et de la Fédération de Russie, a adopté un certain nombre de principes juridiques ainsi qu'un plan d'action commun pour lutter contre ce qu'il appelle la criminalité technologique.[7] Il prévoit notamment une coopération entre les services de répression sur le plan pratique ainsi que certaines modalités d'entraide judiciaire. Parmi les formes de coopération examinées on citera:

a) La coopération en vue d'équiper et de former le personnel des services de répression, afin que ceux-ci disposent d'effectifs en nombre suffisant, qualifiés et dotés des compétences techniques requises;

b) La coopération dans l'élaboration de normes techniques pour la recherche et l'authentification des données électroniques.

50. Afin de faciliter l'exécution rapide d'une demande d'entraide émanant d'un État, le Groupe des Huit a décidé de créer un réseau de points de contact, disponibles 24 heures sur 24 et sept jours sur sept. Ces points de contact, qui sont déjà en place, sont chargés de tâches très diverses. Si on lui en fait la demande, un point de contact fournira des données concrètes qui permettront peut-être d'élargir l'enquête à l'autre État ou de solliciter son aide, prendra toutes les autres mesures nécessaires pour répondre au plus vite à une demande officielle d'entraide judiciaire ou prendra des mesures conservatoires, dans la mesure où le droit interne le permet, dans l'attente de cette demande. Ces points de contact n'existent pas uniquement dans les pays du Groupe des Huit: bien d'autres États en ont également mis en place chez eux de leur propre initiative. Dans certains pays, la création de ces groupes de spécialistes peut s'avérer impossible faute de compétences techniques ou de moyens financiers. Dans d'autres États, la lutte contre la cybercriminalité peut revêtir une importance moindre. Il va de soi que plus nombreux seront les États qui forment et équipent un personnel qui sera disponible 24 heures sur 24 et sept jours sur sept, plus le système gagnera en efficacité.

51. Dans le cadre d'Interpol, plusieurs groupes d'experts sur la criminalité en rapport avec les technologies de l'information ont été constitués. Le Groupe de travail européen sur la criminalité liée aux technologies de l'information a mis au point un guide sur la criminalité informatique disponible sur CD-ROM, qui contient des instructions sur les modalités d'enquête concernant les délits informatiques, une description des outils et des techniques permettant de rechercher et d'obtenir des documents électroniques, ainsi que des informations sur les dispositions pertinentes du droit matériel positif et du droit procédural de différents pays. Les groupes de travail s'occupent de la mise au point de logiciels spécifiques permettant de détecter certains délits sur Internet. Plusieurs stages de formation ont été organisés à l'intention des agents enquêtant sur la criminalité informatique.

52. Le manuel sur la prévention et la répression de la criminalité informatique, publié par l'ONU, vise à harmoniser le droit positif et le droit procédural, de même qu'à favoriser la coopération internationale dans la lutte contre la criminalité informatique. Il contient un chapitre sur la sécurité des données et un sur la prévention de la cybercriminalité.[8]

53. Tant les stratégies fondées sur la coopération que celles reposant sur l'initiative d'un individu ou d'un État sont utiles. Aussi importe-t-il de tirer le meilleur parti possible des unes et des autres. À cet égard, il est nécessaire d'organiser régulièrement des réunions internationales dans lesquelles les services s'occupant de cybercriminalité pourront se rencontrer et échanger des informations pratiques et des données d'expérience. D'autres structures permanentes, telles que les banques de données, les sites Web et les groupes de discussion, contribueront à améliorer l'échange d'informations.[9]

54. Un troisième volet du plan d'action du Groupe des Huit concerne la coordination de la coopération entre les milieux industriels et l'État. Il y est question:

a) D'encourager les organismes de normalisation à élaborer des normes tendant à assurer la fiabilité et la sécurité des technologies de télécommunication et de traitement des données;

b) De concevoir des systèmes d'information et de télécommunication pouvant détecter toute utilisation abusive des réseaux informatiques, d'en retrouver l'auteur et de recueillir les éléments de preuve nécessaires.

Étant donné que les enquêtes criminelles dans un environnement informatique peuvent être contraignantes pour les entreprises, la coopération et la concertation avec ces dernières sont importantes, voire nécessaires dans de nombreux domaines allant de la sécurité des données et de la mise au point de produits à l'exécution des ordonnances judiciaires. Les négociations entre les pouvoirs publics et les organisations industrielles peuvent aboutir à des arrangements sectoriels ou d'autres accords de caractère facultatif ou obligatoire.

B. Traités d'entraide judiciaire et autres traités internationaux

55. La coopération internationale sous la forme d'une entraide judiciaire exige un accord international ou tout autre instrument similaire, tel qu'une législation réciproque. Ces dispositions, qu'elles soient multilatérales ou bilatérales, font obligation aux autorités d'une partie contractante de donner suite à une demande d'entraide judiciaire dans les cas convenus. Cette demande ne peut être exécutée que si elle est conforme au droit interne de l'État requis ou, faute de règles spécifiques, dans la mesure où elle n'y contrevient pas.

56. Les États coopèrent plus efficacement en matière pénale s'ils ont un point commun, par exemple s'ils ont une législation ou un code pénal similaire et s'ils appliquent le droit pénal de la même manière. Dans nombre de conventions internationales se rapportant aux questions pénales, ce point commun est la règle de la double incrimination. Un État ne peut coopérer avec un autre État dans une enquête et des poursuites concernant des actes qui ne sont pas criminalisés dans l'État requis. L'absence de cette règle dans des conventions anciennes constitue par conséquent un motif valable pour refuser d'aider un État. Les conventions plus récentes n'imposent pas cette condition de forme mais font référence au caractère raisonnable ou non de la demande. On peut, en effet, considérer qu'il n'est pas raisonnable d'exécuter une demande d'entraide judiciaire si, par exemple, celle-ci vise une infraction mineure ou concerne un comportement qui ne constitue pas une infraction dans l'État requis.

57. Un moyen d'améliorer la coopération internationale en matière pénale consiste donc à harmoniser certaines dispositions de fond du droit pénal. Les différences culturelles, sociales et économiques entre États peuvent donner lieu à des politiques pénales différentes. À cet égard, il est probablement moins difficile de mener des travaux au niveau international pour harmoniser les dispositions sur les atteintes à la confidentialité, à l'intégrité et à la disponibilité des données (voir par. 15), telles que les dispositions concernant les aspects techniques, que de vouloir harmoniser les dispositions sur les infractions en rapport avec le contenu, en raison de leur impact sur les droits de l'homme (notamment la liberté d'expression). La pornographie impliquant des enfants, qui, de l'avis de tous, doit être combattue, semble être l'exception qui confirme la règle.

58. L'entraide judiciaire désigne ici toute forme d'assistance juridique, généralement en rapport avec l'exercice de certains pouvoirs de contrainte dans le cadre d'enquêtes sur la cybercriminalité. Outre l'aide traditionnelle, telle que l'audition des témoins, la demande a pour but d'obtenir certaines données qui sont stockées sur un système informatique situé sur le territoire d'un autre État, ou qui sont transférées électroniquement par un réseau et peuvent être surveillées ou interceptées sur le territoire de cet État.

59. Les États déterminent dans leur droit interne les pouvoirs qui peuvent être mis en œuvre afin d'aider d'autres États signataires. Ils ne proposeront pas nécessairement d'exercer tous leurs pouvoirs internes dans le cadre de leur collaboration à l'enquête menée par d'autres États signataires. Parfois, compte tenu des intérêts communs des États concernés, ils fourniront une assistance dans un cas précis, au lieu de le faire de manière régulière ou systématique. Par ailleurs, l'entraide judiciaire, qui relève du droit international, est avant tout régie par le principe de réciprocité. C'est notamment pour cette raison que les États négociant la portée de l'entraide judiciaire avec d'autres peuvent hésiter à aller aussi loin que leur législation interne le leur permettrait. La règle de la double incrimination – règle selon laquelle l'acte visé dans la demande d'entraide doit constituer une infraction dans les deux États concernés – peut également être invoquée, directement ou indirectement, comme motif de refus de l'entraide judiciaire. En outre, les accords internationaux d'entraide judiciaire prévoient parfois des cas où l'entraide ne sera pas accordée. Sont généralement exclus certains types d'infractions, notamment fiscales, politiques ou militaires, et les infractions qui ne sont pas considérées comme suffisamment graves (au regard des peines encourues) pour justifier un tel effort.

60. D'autres problèmes peuvent se poser en rapport avec l'entraide judiciaire dans les enquêtes sur la cybercriminalité internationale. Si un État partie n'a prévu dans son droit interne aucune disposition spécifique autorisant la recherche d'éléments de preuve dans un environnement électronique, il ne sera peut-être pas en mesure de répondre à une demande d'entraide ou d'y répondre dûment. Aussi l'harmonisation des pouvoirs de contrainte joue-t-elle un rôle important dans la coopération internationale.

61. En outre, il est probable que l'entraide judiciaire revête un caractère plus urgent dans les affaires de cybercriminalité que dans les enquêtes traditionnelles du fait que les éléments de preuve électroniques risquent d'être perdus s'ils ne sont pas rapidement sauvegardés. Toutefois, il ne sera pas toujours possible d'agir immédiatement pour des raisons de forme et d'ordre pratique. Par exemple, les mesures à prendre exigent

parfois qu'une ordonnance judiciaire soit rendue dans l'État requis. Afin d'éviter la disparition d'éléments de preuve dans ces situations, on pourrait mettre en place un dispositif permettant de prendre rapidement des mesures conservatoires exigeant le moins de formalités possibles, puis d'engager des procédures plus traditionnelles une fois obtenus les éléments de preuve, afin de déterminer si ceux-ci doivent être communiqués à l'État requérant. Dans un tel dispositif, la législation interne autoriserait non seulement l'obtention de données en réponse à une demande informelle mais également leur conservation jusqu'à ce que leur communication soit officiellement demandée au titre de l'accord d'entraide judiciaire. Si une telle demande n'était pas reçue en temps voulu ou était jugée irrecevable, les données ainsi sauvegardées seraient effacées. Un dispositif similaire est envisageable pour la conservation de données de trafic détenues par les opérateurs de systèmes de télécommunication et les fournisseurs de services sur Internet.

62. Les réseaux informatiques internationaux permettent de réaliser sur un territoire donné des activités qui peuvent (de manière délibérée ou involontaire) produire des effets extraterritoriaux. Par exemple, les services de répression d'un État pourraient obtenir des données sur un réseau informatique en effectuant une perquisition informatique légale dans cet État et constater que certaines des données obtenues avaient été stockées sur une partie du réseau située dans un autre État et qu'elles sont protégées par les lois de ce dernier. De même, un État pourrait légalement intercepter des communications électroniques traversant son territoire, même si les personnes communiquant entre elles se trouvent dans d'autres États où elles jouissent d'une protection juridique contre toute immixtion arbitraire dans leurs communications privées. Les agents des services de répression intervenant sur un réseau pourraient également faire office d'agents d'infiltration conformément à la législation de leur État lorsque leurs agissements ou leurs méthodes ne sont pas autorisés par le droit des États où ils opèrent. Tous ces scénarios sont inédits et uniques et le droit international ne fournit actuellement guère d'indications ou d'orientations pour résoudre les problèmes qui en découlent.

63. À l'heure actuelle, aucun consensus non plus ne s'est dégagé quant aux solutions qui pourraient être apportées au problème des effets transfrontières des mesures d'enquête internes appliquées en toute légalité. Il est généralement admis qu'un État est autorisé par la loi à appliquer des mesures d'enquête ou à exercer des pouvoirs de contrainte à l'égard de l'un quelconque de ses citoyens à l'intérieur de son propre territoire, sur lequel il exerce une compétence exclusive. De l'exercice de ces pouvoirs il se peut que des données se trouvant ailleurs soient recherchées, copiées voire effacées, ce qui, pour l'État où la recherche est effectuée, peut constituer une infraction au sens de son droit pénal et une violation de sa souveraineté nationale. D'un autre côté toutefois, 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 se trouvent 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.

64. S'agissant de la 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 différentes concernant l'état du droit international en la matière méritent d'etre 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 problèmes pratiques que posent les enquêtes sur les délits informatiques.

65. Selon 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.

66. La communauté internationale pourrait trouver de nouvelles idées pour établir une règle de droit sur la

manière de définir les droits des États concernant l'utilisation commune des réseaux informatiques, que ceux-ci soient terrestres ou mobiles ou qu'ils fassent appel aux satellites. Entre-temps, une solution pragmatique pourrait être adoptée d'un commun accord sous la forme d'un traité ou d'un autre instrument international qui décrivait certaines procédures permettant d'établir un équilibre judicieux entre les intérêts de l'État effectuant la recherche et ceux de l'État visé par la recherche et de ses résidents.

VI. Conclusion

67. Face à la multiplication des délits liés à l'utilisation du réseau informatique que facilite l'établissement de vastes réseaux électroniques internationaux et publics, la coordination et la coopération internationales sont devenues essentielles pour en venir à bout. Les principes fondamentaux de cette coordination et coopération sont les suivants:

a) *La sensibilisation de l'opinion publique*. Elle peut contribuer à réduire le nombre de délits commis dans l'environnement électronique. Les industriels – fabricants de matériel et de logiciels, prestataires de services et autres – de même que les organisations de consommateurs et les pouvoirs publics peuvent ensemble informer le public sur la sécurité et les risques afférents aux environnements électroniques ouverts et les conseiller sur la manière de protéger leurs intérêts;

b) *L'élaboration de politiques communes en matière de cybercriminalité*. La criminalité informatique revêtant un caractère transnational, toute stratégie de répression passe par l'élaboration de politiques communes sur les questions clefs, par exemple la prévention de la constitution de "paradis informatiques" dans les États où certaines activités ne sont pas tenues pour des infractions pénales. La mise au point de ces politiques pourrait s'inscrire dans le cadre du Programme des Nations Unies pour la prévention du crime et la justice pénale et venir étayer les travaux déjà entrepris par d'autres organisations internationales;

c) *L'amélioration des méthodes d'enquête*. Il conviendrait de prendre des mesures efficaces afin de renforcer les moyens d'enquête dans les réseaux informatiques, en particulier dans les cas où plusieurs compétences interviennent. Il faut notamment pouvoir agir rapidement pour empêcher que des éléments de preuve disparaissent ou deviennent inaccessibles. Les perquisitions dans les systèmes informatiques et la surveillance des réseaux informatiques peuvent exiger de nouveaux pouvoirs que la procédure pénale traditionnelle ne prévoit pas actuellement. Par ailleurs, la quantité de données emmagasinées dans un système informatique et la facilité avec laquelle les enquêteurs peuvent y accéder soulèvent d'importants problèmes touchant la protection de la vie privée et d'autres problèmes connexes tout aussi sérieux. La conception et l'exercice de ces nouveaux pouvoirs devront tenir compte, dans un souci d'équilibre judicieux, des droits inhérents à la personne humaine;

d) Les enquêtes sur la cybercriminalité exigent non seulement des effectifs possédant des connaissances scientifiques et techniques particulières, mais également la mise en place de procédures spécifiques, ce qui suppose l'élaboration de programmes de formation et la conception de logiciels pour les enquêtes. Des programmes internationaux de formation devraient être élaborés et les États devraient mettre en commun leurs connaissances techniques. L'ONU, dans le cadre de son programme pour la prévention du crime et la justice pénale, pourrait examiner l'opportunité de revoir son manuel sur la criminalité informatique et étoffer ainsi les travaux déjà entrepris par d'autres organisations internationales;

e) *L'amélioration de la coordination et de l'assistance entre les pays*. Les cyberdélits sont commis dans les environnements électroniques de dimension mondiale et ne se confinent pas nécessairement au territoire d'un État donné. Afin d'enquêter avec efficacité sur eux, les États peuvent avoir besoin de l'aide d'autres États. Cette aide englobe à la fois la coopération officieuse d'agents des services de répression et l'entraide judiciaire officielle des autorités centrales. Cette aide doit pouvoir être fournie d'autant plus rapidement et efficacement que, contrairement à ce qui se passe dans le cas de nombreuses autres infractions en l'espèce, les données des réseaux informatiques peuvent aisément disparaître. Pour être efficace, cette assistance s'appuierait sur les dispositions suivantes:

i) La mise en place de points de contact comme ceux créés par le Groupe des Huit, afin d'informer les États requérants de l'aide qu'ils peuvent recevoir et d'appliquer les mesures nécessaires pour exécuter les demandes dans la mesure où le droit interne le permet;

ii) L'examen des systèmes d'entraide judiciaire dans le contexte de la cybercriminalité. Il y a lieu d'étudier les critères et les pratiques classiques en matière d'assistance judiciaire de manière à déterminer s'ils répondent aux besoins des enquêtes sur la cybercriminalité contemporaine et de définir les

améliorations qui pourraient y être apportées. Il faudrait s'intéresser à l'adéquation en général des pouvoirs en matière d'enquêtes criminelles faisant intervenir des réseaux informatiques et explorer la possibilité de prendre promptement des mesures qui permettent d'obtenir et de préserver des données dans le cadre des enquêtes criminelles conduites dans d'autres États.

Notes

[1] Au nombre des associations ou sociétés de ce type figurent par exemple la United States Internet Providers Association (USIPA), la Canadian Association of Internet Providers (CAIP) et l'association paneuropéenne des associations de fournisseurs d'accès à Internet (EuroISPA). Il existe aussi des associations nationales dans certains pays d'Europe, notamment l'Allemagne, la Belgique, l'Espagne, la France, l'Italie, les Pays-Bas et le Royaume-Uni de Grande-Bretagne et d'Irlande de Nord.

[2] http://www.nua.ie/surveys/how-many-online, 18 octobre 1999.

[3] Voir les définitions techniques des données de l'Organisation internationale de normalisation.

[4] *La fraude liée à l'informatique: Analyse des politiques juridiques*, Série PIIC n° 10, 1986.

[5] Conseil de l'Europe (1989), recommandation n° R (89) 9.

[6] "Global Information Networks: Realising the Potential", Conférence ministérielle, Bonn, juillet 1997.

[7] Voir le communiqué publié à l'issue de la réunion des Ministres de la justice et de l'intérieur du Groupe des Huit, tenue à Washington, les 9 et 10 décembre 1997 (http://www.usdoj.gov/criminal/cybercrime/communique.htm). Le plan d'action a été approuvé par les chefs d'État et de gouvernement en 1998 et recommandé à d'autres organisations internationales telles que l'Organisation des États américains et l'Union européenne.

[8] *Revue internationale de politique criminelle*, nos 43/44, 1994 (publication des Nations Unies, numéro de vente: F.94.IV.5).

[9] Par exemple les deux sites suivants: World Justice Information Network (http://www.justinfo.net) et Police Officer Internet Directory (http://www.officer.com/c_crimes.htm).